IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

WESERVE ACCESS, LLC, Plaintiff, v. BIRCH GROVE SOFTWARE, INC. d/b/a ACTIVTRAK, Defendant.	CIVIL ACTION NO. 6:21-cv-00238 ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT JURY TRIAL DEMANDED

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Weserve Access, LLC ("Weserve" or "Plaintiff") files this original complaint against Birch Grove Software, Inc. d/b/a ActivTrak ("Defendant") alleging, based on its own knowledge as to itself and its own actions, and based on information and belief as to all other matters, as follows:

PARTIES

1. Weserve Access, LLC is a Texas corporation, with its principal place of business at 1916 Wimberly Lane, Austin, Texas 78735.

2. Defendant, Birch Grove Software, Inc. d/b/a ActivTrak, is a company organized and existing under the laws of Delaware with a place of business in this district at 1301 South Mopac Expressway, Suite LL25, Austin, Texas 78746.

3. Defendant may be served at its registered agent for service of process, CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

JURISDICTION AND VENUE

4. This is an action for infringement of United States patents arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of the action under 28 U.S.C. § 1331 and § 1338(a).

5. Venue is proper in this district pursuant to 28 U.S.C. §§ 1400(b) and 1391(c). Defendant has a place of business in this district, including at 1301 South Mopac Expressway, Suite LL25, Austin, Texas 78746, and has committed acts of infringement in this district.

6. Defendant is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to Defendant's substantial business in this forum, including (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this district.

7. Specifically, Defendant intends to do and does business in Texas, directly or through intermediaries, and offers its products and/or services, including those accused herein of infringement, to customers and potential customers located in the forum state, including in this district.

THE TECHNOLOGY

8. The patents-in-suit, U.S. Patent Nos. 6,978,304 (the "'304 Patent"), 7,634,571 (the "'571 Patent"), 7,958,237 (the "'237 Patent"), and 8,930,535 (the "'535 Patent") (collectively the "Asserted Patents"), teach methods for controlling a computer's web browser, remotely monitoring an internet session, and managing computer network access. Specifically, these patented methods aid in determining a computer user's Internet and network activity.

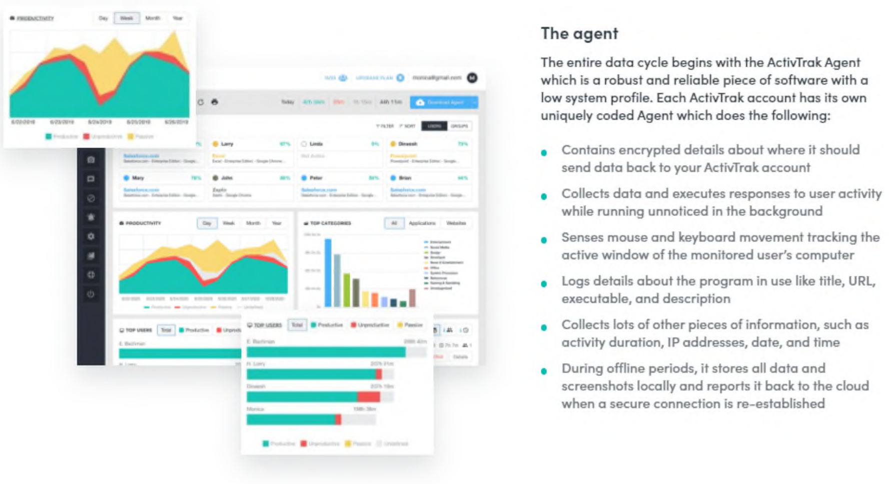
9. Inventors David Fertell ("Fertell") and Joe Field ("Field") pioneered the field of remotely monitoring online computer activity and started Pearl Software, Inc. in 1996. Recognizing how inappropriate material accessible on the Internet presents risks to children, employers, and organizations, Fertell and Field developed efficient and reliable methods of monitoring and controlling Internet activity. Their work received many accolades from the technical press and civic leaders such as the White House's Internet Taskforce.

10. The Patent Office issued Fertell and Field several patents in the field including the Asserted Patents. For years, Pearl Software and Fertell worked hard, expending significant resources to develop the market for Internet activity monitoring and control software in schools, libraries, public organizations, private companies, government and law enforcement agencies and homes.

11. The inventors attended trade shows, spoke at conferences, appeared on television and radio shows, supported Internet safety not-for-profit organizations, and published articles and guides about the risks of unmonitored computer access in organizations and at home. As a result of Fertell's and Pearl's efforts, Pearl Software became the industry experts, garnering praise and awards from industry publications such as an Editor's Choice award from PC Magazine.

THE ACCUSED INSTRUMENTALITIES

12. On information and belief, Defendant made, had made, used, imported, provided, supplied, distributed, sold, or offered to sell products and/or systems, including its computing infrastructure to provide ActivTrak monitoring software (the "Accused Instrumentalities").



The agent

The entire data cycle begins with the ActivTrak Agent which is a robust and reliable piece of software with a low system profile. Each ActivTrak account has its own uniquely coded Agent which does the following:

- Contains encrypted details about where it should send data back to your ActivTrak account
- Collects data and executes responses to user activity while running unnoticed in the background
- Senses mouse and keyboard movement tracking the active window of the monitored user's computer
- Logs details about the program in use like title, URL, executable, and description
- Collects lots of other pieces of information, such as activity duration, IP addresses, date, and time
- During offline periods, it stores all data and screenshots locally and reports it back to the cloud when a secure connection is re-established

13. On information and belief, Defendant provides the Accused Instrumentalities to users through its websites, including activtrak.com.

14. On information and belief, Defendant also provides the Accused Instrumentalities for delivery to mobile applications for Apple iOS devices and Android devices.

COUNT I: INFRINGEMENT OF U.S. PATENT NO. 6,978,304

Direct Infringement

15. Plaintiff repeats and re-alleges the allegations in Paragraphs 1-14 as if fully set forth in their entirety.

16. On December 20, 2005, the ’304 Patent was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Method of Remotely Monitoring an Internet Session.”

17. Exhibit A is a true and correct copy of the ’304 Patent.

18. Plaintiff is the owner of the ’304 Patent, with all substantial rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the ’304 Patent against infringers, and to collect damages for all relevant times.

19. The ’304 Patent describes novel and non-obvious methods of remotely monitoring an Internet session.

20. The claims of the ’304 Patent are not directed to an abstract idea.

21. For example, Claim 1 is a technical improvement over prior-art methods of remotely monitoring an exchange of data between a local computer and a remote computer.

22. Claim 1 recites “remotely monitoring an exchange of data between a local computer and a remote computer during an Internet session over the Internet.” The “first Internet session” is initiated “between the local computer and a remote computer via the Internet.” Then, after other steps, at least one “Internet server address” and “port number” are transmitted “from the monitor computer to the local computer.” Claim 1 does not recite an abstract idea because it recites specific conditions during computer use and recites specific actions performed “between the local computer and a remote computer” in response to specific conditions being met.

23. Prior-art systems and methods did not include the ability to capture the content of an ongoing Internet communication for display and/or storage.

24. Regardless of whether Claim 1 is directed to an abstract idea, Claim 1 recites patentable subject matter because it recites an inventive concept.

25. For example, the capturing content of an ongoing Internet communication was not a well-understood practice, routine, or conventional; rather it represents an improvement to computing technology that allows for superior security for online communications and this capturing process did not exist in the prior art.

26. Moreover, the use of the components recited in Claim 1 was, at the time of the invention, unconventional; therefore, Claim 1 recites an inventive concept.

27. The written description of the ’304 Patent describes in technical detail each of the limitations of the claims, allowing a skilled artisan to understand the scope of the claims and how the non-conventional and non-generic combination of claim limitations is patentably distinct from and improved upon what may have been considered conventional or generic in the art at the time of the invention.

28. Defendant made, had made, used, imported, provided, supplied, distributed, sold, or offered to sell the Accused Instrumentalities.

29. Defendant has infringed, and continues to infringe, the ’304 Patent by making, having made, using, importing, providing, supplying, distributing, selling, or offering to sell the Accused Instrumentalities. Defendant’s infringement of the ’304 Patent includes, for example, but is not limited to, its use and testing of the Accused Instrumentalities.

30. On information and belief, Defendant directs and controls its customers to install the Accused Instrumentalities through its websites, including activtrak.com.

31. On information and belief, Defendant also directs and controls its customers to install and use the Accused Instrumentalities through respective application stores for its mobile applications for Apple iOS devices and Android devices.

32. By doing so, Defendant directs or controls its customers to infringe the ’304 Patent by making, having made, using, importing, providing, supplying, distributing, selling, or offering to sell the Accused Instrumentalities in an infringing manner.

33. Defendant, through its own use and testing or its direction and control of its customers, has directly infringed (literally and/or under the doctrine of equivalents) at least Claim 1 of the ’304 Patent. Its infringement in this regard is ongoing.

34. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control collect information such as activity duration, IP addresses, date, and time. The Accused Instrumentalities remotely monitor an exchange of data between a local computer and a remote computer during an Internet session over the Internet.

35. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control store at their local computer an Internet server address and port number of a monitor computer under the control of Defendant.

36. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control initiate a first Internet session between their local computer and a remote computer, such as a website, via the Internet. The Accused Instrumentalities further store data associated with the first Internet session on the local computer.

37. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control retrieve the Internet server address and port number stored at their local computer, and use the Internet server address and port number, concurrent with the first Internet session, to initiate a second Internet session between their local computer and the monitor computer under the control of Defendant.

38. Defendant transmits another Internet server address and port number from its monitor computer to the Accused Instrumentalities.

39. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control terminate the second Internet session.

40. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control initiate a third Internet session between their local computer

and the monitor computer under the control of Defendant. The third Internet session is initiated using the other Internet server address and/or the other port number.

41. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control transfer from their local computer to the monitor computer (under the control of Defendant) via the third Internet session the stored data associated with the first Internet session, including, for example, but not limited to, information about the website that was part of the first Internet session.

42. Plaintiff has been damaged as a result of the infringing conduct by Defendant or Defendant's customers under Defendant's control alleged above. Thus, Defendant is liable to Plaintiff in an amount that adequately compensates it for such infringements, which by law cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

43. Plaintiff and/or its predecessors-in-interest have satisfied all statutory obligations required to collect pre-filing damages for the full period allowed by law for infringement of the '304 Patent.

Indirect Infringement

44. Plaintiff repeats and re-alleges the allegations in Paragraphs 1-43 as though fully set forth in their entirety.

45. Defendant has also indirectly infringed the '304 Patent, at least since the filing of this complaint, by inducing others to directly infringe the '304 Patent. Defendant has induced others, including its customers, affiliates, third-party manufacturers, shippers, distributors, retailers, or other persons acting on Defendant's or its affiliates' behalf, to directly infringe (literally and/or under the doctrine of equivalents) the '304 Patent by making, having made, using,

importing, providing, supplying, distributing, selling, or offering to sell the Accused Instrumentalities in an infringing manner. Defendant took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to, for example, use the Accused Instrumentalities in a manner that infringes one or more claims of the ’304 Patent or induce others to use the Accused Instrumentalities in a manner that infringes one or more claims of the ’304 Patent, including, for example, Claim 1 of the ’304 Patent. Such steps by Defendant included, among other things, advising or directing others to use the Accused Instrumentalities in an infringing manner; advertising and promoting the use of the Accused Instrumentalities in an infringing manner; and/or distributing instructions that guide others to use, operate, make, or have made the Accused Instrumentalities in an infringing manner. Defendant is performing these steps, which constitute induced infringement, with the knowledge of the ’304 Patent and with the knowledge that the induced acts constitute infringement. Defendant’s inducement is ongoing.

46. Defendant has also indirectly infringed by contributing to the infringement of the ’304 Patent. Defendant has contributed to the direct infringement of the ’304 Patent by its customers, affiliates, or third-party manufacturers, shippers, distributors, retailers, or other persons acting on its or its affiliates’ behalf. The Accused Instrumentalities have special features that are specially designed to be used in an infringing way and that have no substantial uses other than ones that infringe the ’304 Patent, including, for example, Claim 1 of the ’304 Patent. The special features include, for example, the remote monitoring that is used in a manner that infringes the Asserted Patents. The special features constitute a material part of the invention of one or more of the claims of the ’304 Patent and are not staple articles of commerce suitable for substantial non-infringing use. Defendant’s contributory infringement is ongoing.

47. Defendant has knowledge of the ’304 Patent at least as of the date when it was notified of the filing of this action.

48. Defendant’s actions are at least objectively reckless as to the risk of infringing a valid patent and this objective risk was either known or should have been known by Defendant.

49. Defendant’s direct and indirect infringement of the ’304 Patent is, has been, and continues to be willful, intentional, deliberate, and/or in conscious disregard of Plaintiff’s rights under the patent.

50. Plaintiff has been damaged as a result of the infringing conduct by Defendant alleged above. Thus, Defendant is liable to Weserve in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT II: INFRINGEMENT OF U.S. PATENT NO. 7,634,571

Direct Infringement

51. Plaintiff repeats and re-alleges the allegations in Paragraphs 1-50 as if fully set forth in their entirety.

52. On December 15, 2009, the ’571 Patent was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Method of Remotely Monitoring an Internet Session.”

53. Exhibit B is a true and correct copy of the ’571 Patent.

54. Plaintiff is the owner of the ’571 Patent, with all substantial rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the ’571 Patent against infringers, and to collect damages for all relevant times.

55. The ’571 Patent describes novel and non-obvious methods of remotely monitoring an Internet session.

56. The claims of the ’571 Patent are not directed to an abstract idea.

57. For example, Claim 1 is a technical improvement over prior-art methods of remotely monitoring an Internet session.

58. Claim 1 recites “remotely monitoring an Internet session.” The “first Internet session” is initiated “at a first Internet protocol (IP) address.” Data transmitted during the first Internet session is stored in a memory buffer in a user’s computer. Then, after other steps, the user computer transfers “the data stored in the memory buffer.” Claim 1 does not recite an abstract idea because it recites specific conditions during computer use and recites specific actions performed during the Internet session in response to specific conditions being met.

59. Prior-art systems and methods did not include the ability to remotely monitor data associated with an Internet session in the manner recited in the claims of the ’571 Patent.

60. Regardless of whether Claim 1 is directed to an abstract idea, Claim 1 recites patentable subject matter because it recites an inventive concept.

61. For example, the monitoring of data associated with an Internet session was not a well-understood practice, routine, or conventional; rather it represents an improvement to computing technology that allows for superior security for online communications and this monitoring process did not exist in the prior art.

62. Moreover, the use of the steps recited in Claim 1 was, at the time of the invention, unconventional; therefore, Claim 1 recites an inventive concept.

63. The written description of the ’571 Patent describes in technical detail each of the limitations of the claims, allowing a skilled artisan to understand the scope of the claims and how the non-conventional and non-generic combination of claim limitations is patentably distinct from

and improved upon what may have been considered conventional or generic in the art at the time of the invention.

64. Defendant made, had made, used, imported, provided, supplied, distributed, sold, or offered to sell the “Accused Instrumentalities.”

65. Defendant has infringed, and continues to infringe, the ’571 Patent by using the Accused Instrumentalities. Defendant’s infringement of the ’571 Patent includes, for example, but is not limited to, its use and testing of the Accused Instrumentalities.

66. On information and belief, Defendant directs or controls its customers to install the Accused Instrumentalities through its websites, including activtrak.com.

67. On information and belief, Defendant also directs or controls its customers to install and use the Accused Instrumentalities through respective application stores for its mobile applications for Apple iOS devices and Android devices.

68. By doing so, Defendant directs or controls its customers to infringe the ’571 Patent by making, having made, using, importing, providing, supplying, distributing, selling, or offering to sell the Accused Instrumentalities in an infringing manner.

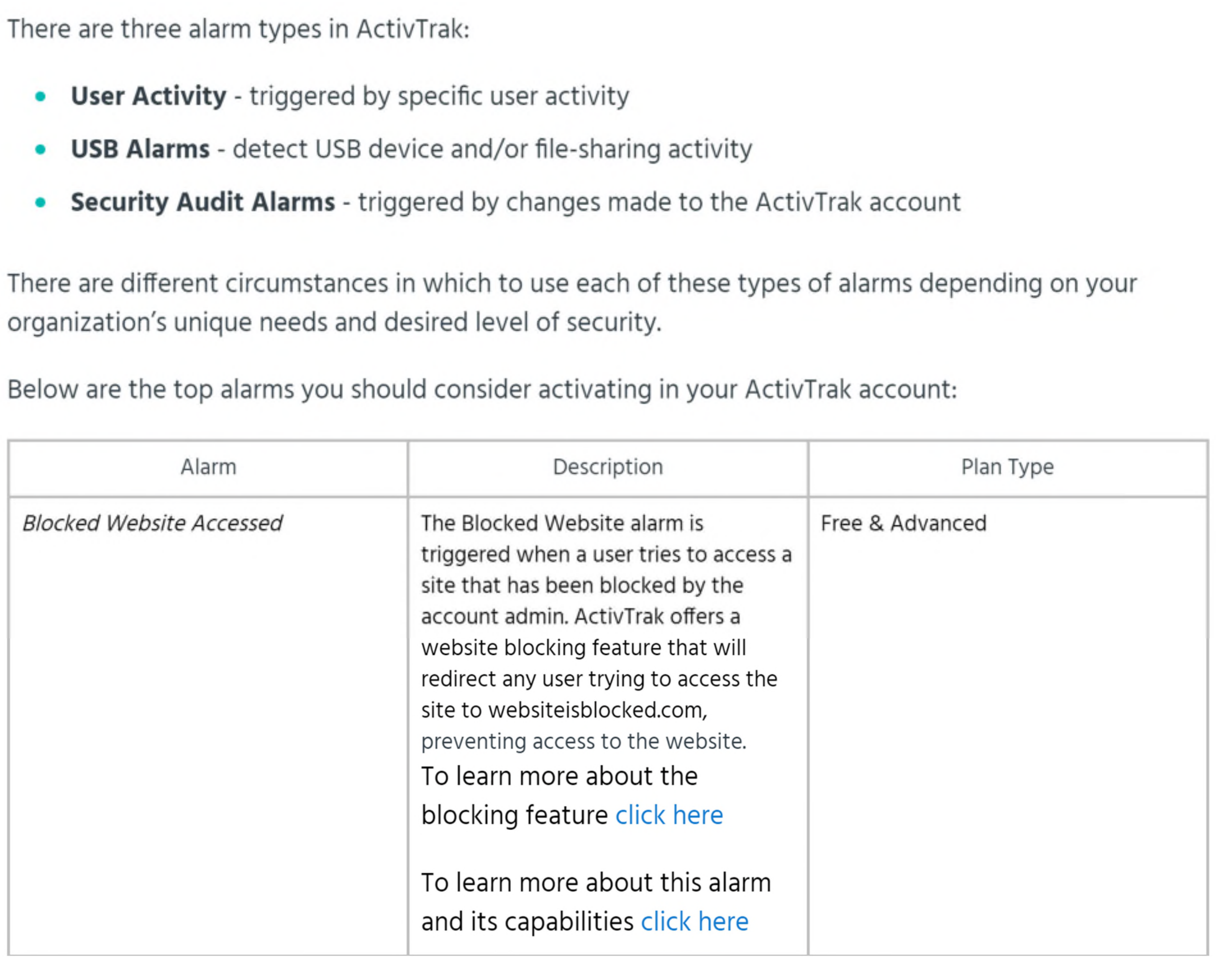
69. Defendant, through its own use and testing or its direction or control of its customers, has directly infringed (literally and/or under the doctrine of equivalents) at least Claim 1 of the ’571 Patent. Defendant’s infringement in this regard is ongoing.

70. Through the Accused Instrumentalities, either Defendant or Defendant’s customers under Defendant’s direction or control collect information such as activity duration, IP addresses, date, and time of various activities of users. The Accused Instrumentalities remotely monitor over the Internet an exchange of data between a local computer and a remote computer during an Internet session.

71. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control participate via computer ("user computer") in a first Internet session at a first Internet protocol (IP) address by, for example, but not limited to, viewing a website.

72. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control store in a memory buffer of the user computer data transmitted from and received at the user computer during the first Internet session at the first IP address. After the data is stored in the user computer, in response to user activation of an icon or key at the user computer, the Accused Instrumentalities initiate a second Internet session at a second IP address, either by Defendant or under the control of Defendant, concurrent with the first Internet session at the first IP address.

73. The Accused Instrumentalities use "Alarms" based on user computer activity, including activation of an icon or key at the user computer. These Alarms include Blocked Website Accessed, Social Media Break, Data Saved to USB Device, File Sharing, Alarm Deleted, ActivTrak User Deleted, Agent Likely Installed. *See* https://support.activtrak.com/hc/en-us/articles/360043204451-Top-User-Alarms-To-Turn-On.



There are three alarm types in ActivTrak:

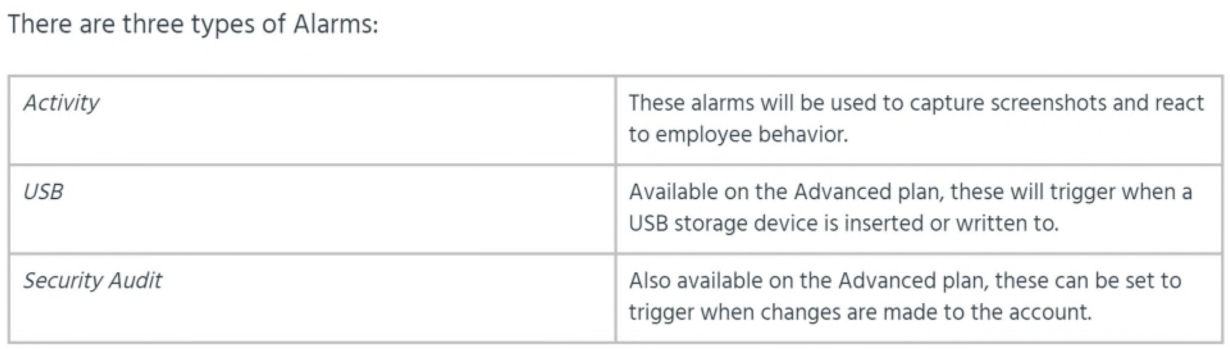
- **User Activity** - triggered by specific user activity
- **USB Alarms** - detect USB device and/or file-sharing activity
- **Security Audit Alarms** - triggered by changes made to the ActivTrak account

There are different circumstances in which to use each of these types of alarms depending on your organization's unique needs and desired level of security.

Below are the top alarms you should consider activating in your ActivTrak account:

Alarm	Description	Plan Type
Blocked Website Accessed	The Blocked Website alarm is triggered when a user tries to access a site that has been blocked by the account admin. ActivTrak offers a website blocking feature that will redirect any user trying to access the site to websiteisblocked.com, preventing access to the website. To learn more about the blocking feature click here To learn more about this alarm and its capabilities click here	Free & Advanced

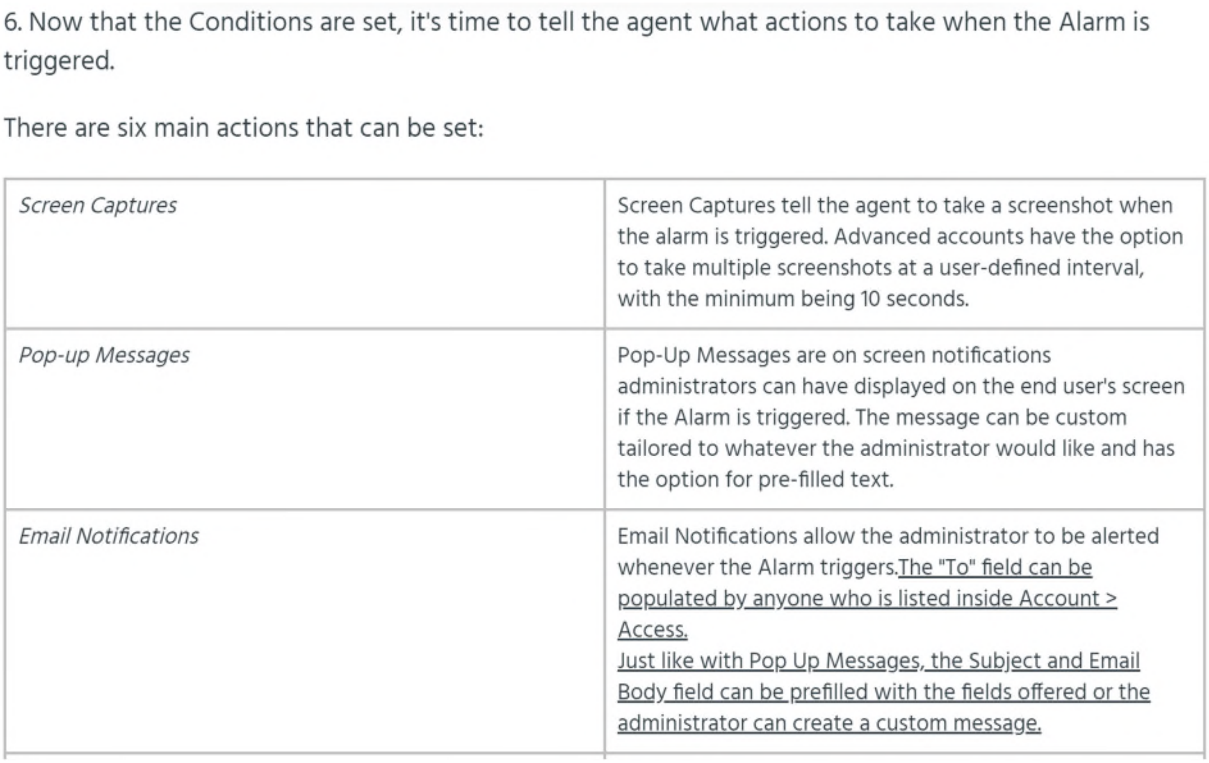
74. The Accused Instrumentalities also provide for user-customized Alarms.



There are three types of Alarms:

Activity	These alarms will be used to capture screenshots and react to employee behavior.
USB	Available on the Advanced plan, these will trigger when a USB storage device is inserted or written to.
Security Audit	Also available on the Advanced plan, these can be set to trigger when changes are made to the account.

75. In the Accused Instrumentalities, with the Custom Alarms, one of six main actions can be set once the Alarm is triggered. These actions include Screen Captures and Email Notifications.



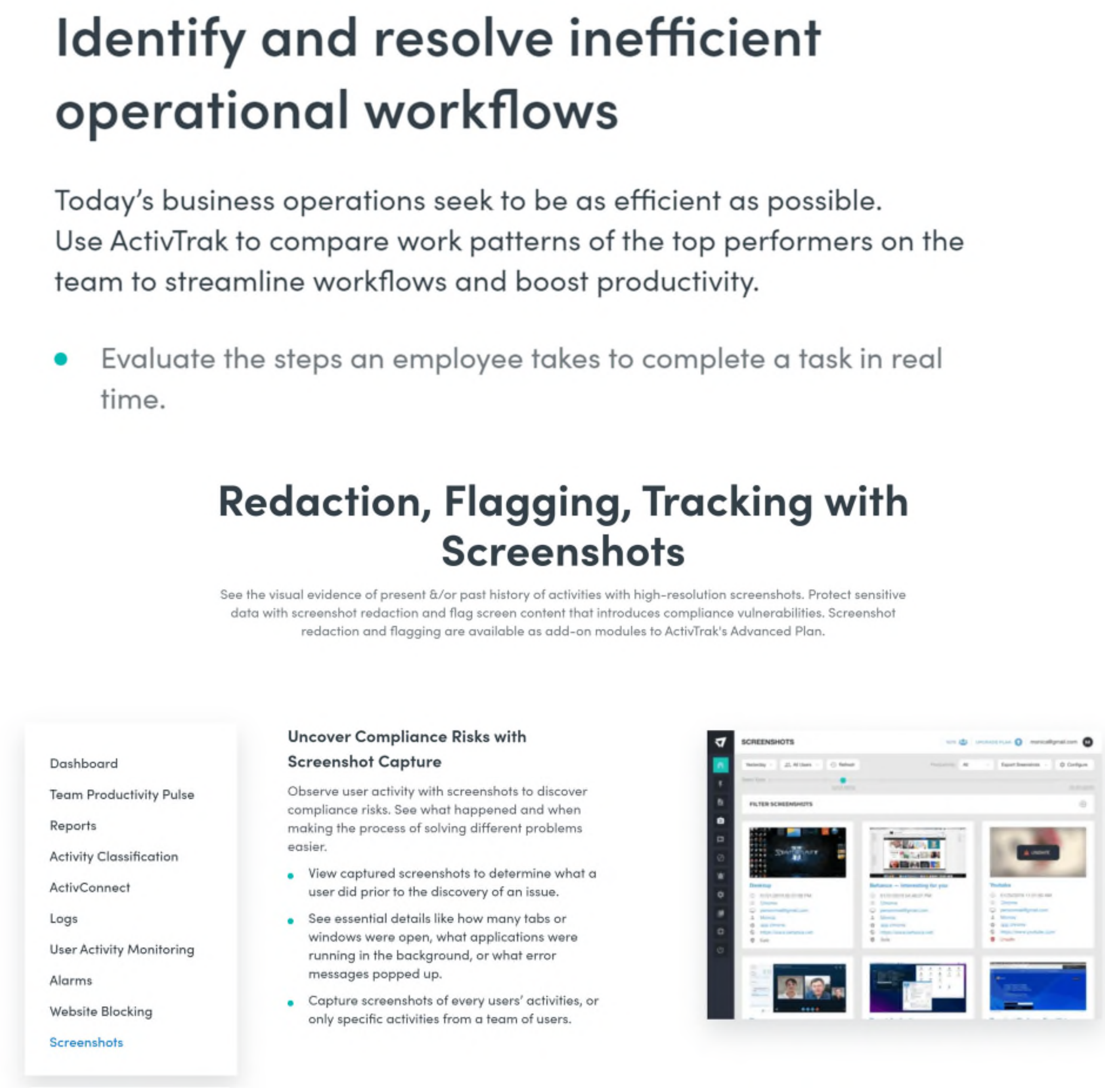
6. Now that the Conditions are set, it's time to tell the agent what actions to take when the Alarm is triggered.

There are six main actions that can be set:

Screen Captures	Screen Captures tell the agent to take a screenshot when the alarm is triggered. Advanced accounts have the option to take multiple screenshots at a user-defined interval, with the minimum being 10 seconds.
Pop-up Messages	Pop-Up Messages are on screen notifications administrators can have displayed on the end user's screen if the Alarm is triggered. The message can be custom tailored to whatever the administrator would like and has the option for pre-filled text.
Email Notifications	Email Notifications allow the administrator to be alerted whenever the Alarm triggers.The "To" field can be populated by anyone who is listed inside Account > Access. Just like with Pop Up Messages, the Subject and Email Body field can be prefilled with the fields offered or the administrator can create a custom message.

76. After initiating the second Internet session, through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control transfer via the user computer the data stored in the memory buffer to the second IP address via the second Internet session, which is controlled by Defendant, via the second Internet session.

77. After initiating the second Internet session, through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control transfer via the user computer data transmitted from and received at the user computer in real-time during the first Internet session to the second IP address via the second Internet session.



Identify and resolve inefficient operational workflows

Today's business operations seek to be as efficient as possible. Use ActivTrak to compare work patterns of the top performers on the team to streamline workflows and boost productivity.

- Evaluate the steps an employee takes to complete a task in real time.

Redaction, Flagging, Tracking with Screenshots

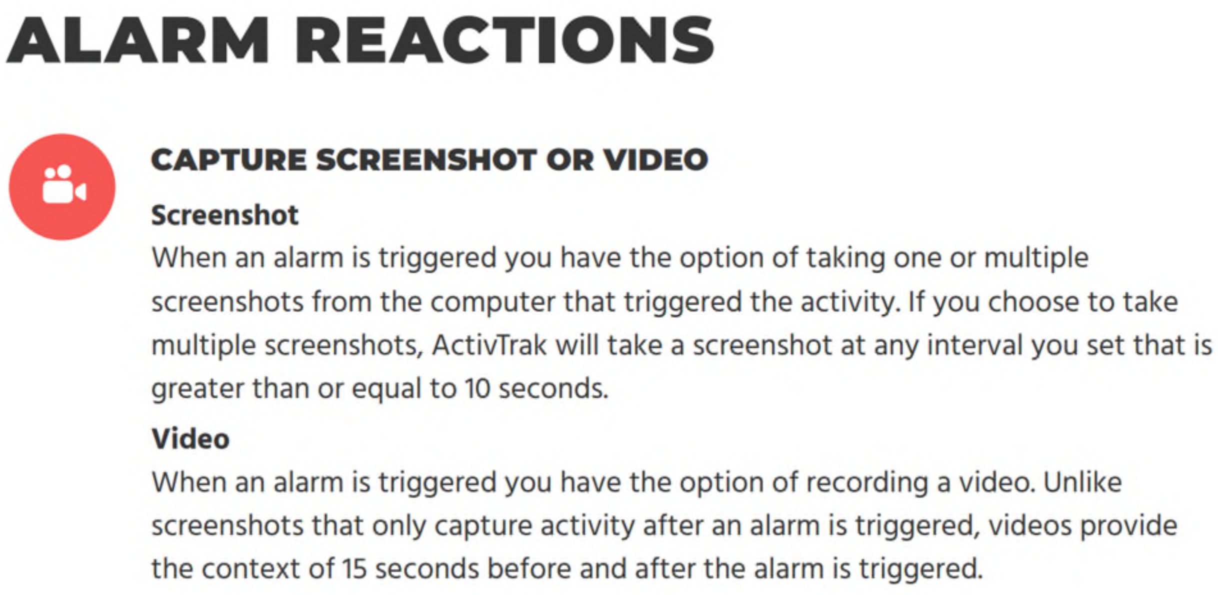
See the visual evidence of present &/or past history of activities with high-resolution screenshots. Protect sensitive data with screenshot redaction and flag screen content that introduces compliance vulnerabilities. Screenshot redaction and flagging are available as add-on modules to ActivTrak's Advanced Plan.

Uncover Compliance Risks with Screenshot Capture

Observe user activity with screenshots to discover compliance risks. See what happened and when making the process of solving different problems easier.

- View captured screenshots to determine what a user did prior to the discovery of an issue.
- See essential details like how many tabs or windows were open, what applications were running in the background, or what error messages popped up.
- Capture screenshots of every users' activities, or only specific activities from a team of users.

See https://activtrak.com/product/screenshots/



ALARM REACTIONS

CAPTURE SCREENSHOT OR VIDEO

Screenshot

When an alarm is triggered you have the option of taking one or multiple screenshots from the computer that triggered the activity. If you choose to take multiple screenshots, ActivTrak will take a screenshot at any interval you set that is greater than or equal to 10 seconds.

Video

When an alarm is triggered you have the option of recording a video. Unlike screenshots that only capture activity after an alarm is triggered, videos provide the context of 15 seconds before and after the alarm is triggered.

See https://3k9e724pnqn2ubftz25jfqs4-wpengine.netdna-ssl.com/wp-content/uploads/2019/08/ALARMS_%E2%80%94new_logo.pdf

78. Plaintiff has been damaged as a result of the infringing conduct by Defendant or Defendant's customers under Defendant's control alleged above. Thus, Defendant is liable to Plaintiff in an amount that adequately compensates it for such infringements, which by law cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

79. Plaintiff and/or its predecessors-in-interest have satisfied all statutory obligations required to collect pre-filing damages for the full period allowed by law for infringement of the '571 Patent.

Indirect Infringement

80. Plaintiff repeats and re-alleges the allegations in Paragraphs 1-79 as though fully set forth in their entirety.

81. Defendant has also indirectly infringed the ’571 Patent, at least since the filing of this complaint, by inducing others to directly infringe the ’571 Patent. Defendant has induced others, including its customers, affiliates, third-party manufacturers, shippers, distributors, retailers, or other persons acting on Defendant’s or its affiliates’ behalf, to directly infringe (literally and/or under the doctrine of equivalents) the ’571 Patent by making, having made, using, importing, providing, supplying, distributing, selling, or offering to sell the Accused Instrumentalities in an infringing manner. Defendant took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to, for example, use the Accused Instrumentalities in a manner that infringes one or more claims of the ’571 Patent or induce others to use the Accused Instrumentalities in a manner that infringes one or more claims of the ’571 Patent, including, for example, Claim 1 of the ’571 Patent. Such steps by Defendant included, among other things, advising or directing others to use the Accused Instrumentalities in an infringing manner; advertising and promoting the use of the Accused Instrumentalities in an infringing manner; and/or distributing instructions that guide others to use, operate, make, or have made the Accused Instrumentalities in an infringing manner. Defendant is performing these steps, which constitute induced infringement, with the knowledge of the ’571 Patent and with the knowledge that the induced acts constitute infringement. Defendant’s inducement is ongoing.

82. Defendant has also indirectly infringed by contributing to the infringement of the ’571 Patent. Defendant has contributed to the direct infringement of the ’571 Patent by its customers, affiliates, or third-party manufacturers, shippers, distributors, retailers, or other persons acting on its or its affiliates’ behalf. The Accused Instrumentalities have special features that are specially designed to be used in an infringing way and that have no substantial uses other than ones that infringe the ’571 Patent, including, for example, Claim 1 of the ’571 Patent. The special

features include, for example, the remote monitoring that is used in a manner that infringes the Asserted Patents. The special features constitute a material part of the invention of one or more of the claims of the ’571 Patent and are not staple articles of commerce suitable for substantial non-infringing use. Defendant’s contributory infringement is ongoing.

83. Defendant has knowledge of the ’571 Patent at least as of the date when it was notified of the filing of this action.

84. Defendant’s actions are at least objectively reckless as to the risk of infringing a valid patent and this objective risk was either known or should have been known by Defendant.

85. Defendant’s direct and indirect infringement of the ’571 Patent is, has been, and continues to be willful, intentional, deliberate, and/or in conscious disregard of Plaintiff’s rights under the patent.

86. Plaintiff has been damaged as a result of the infringing conduct by Defendant alleged above. Thus, Defendant is liable to Weserve in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT III: INFRINGEMENT OF U.S. PATENT NO. 7,958,237

Direct Infringement

87. Plaintiff repeats and re-alleges the allegations in Paragraphs 1-86 as if fully set forth in their entirety.

88. On June 7, 2011, the ’237 Patent was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Method for Managing Computer Network Access.”

89. Exhibit C is a true and correct copy of the ’237 Patent.

90. Plaintiff is the owner of the ’237 Patent, with all substantial rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the ’237 Patent against infringers, and to collect damages for all relevant times.

91. The ’237 Patent describes novel and non-obvious methods of remotely monitoring an Internet session.

92. The claims of the ’237 Patent are not directed to an abstract idea.

93. For example, Claim 1 is a technical improvement over prior-art methods of managing computer network access.

94. Claim 1 recites “controlling computer network access.” A “first communication session” is initiated “at a client computer.” From that “first communication session,” the client computer receives “a second network address.” The client computer initiates a “second communication session” at the second network address, which it uses to receive “an access configuration including a control setting for at least one communication protocol capable of being utilized during a third communication session.” The client computer controls “the conveyance of data” using the “control setting” included in the “access configuration.” Claim 1 does not recite an abstract idea because it recites specific conditions during computer use and recites specific actions performed during the internet session in response to specific conditions being met.

95. Prior-art systems and methods did not include the ability to manage computer network access as recited in, for example, Claim 1.

96. Regardless of whether Claim 1 is directed to an abstract idea, Claim 1 recites patentable subject matter because it recites an inventive concept.

97. For example, the patented method for managing computer network access was not a well-understood practice, routine, or conventional; rather it represents an improvement to

computing technology that allows for superior security for online communications that did not exist in the prior art.

98. Moreover, the use of the components recited in Claim 1 was, at the time of the invention, unconventional; therefore, Claim 1 recites an inventive concept.

99. The written description of the ’237 Patent describes in technical detail each of the limitations of the claims, allowing a skilled artisan to understand the scope of the claims and how the non-conventional and non-generic combination of claim limitations is patentably distinct from and improved upon what may have been considered conventional or generic in the art at the time of the invention.

100. Defendant made, had made, used, imported, provided, supplied, distributed, sold, or offered to sell the Accused Instrumentalities.

101. Defendant has infringed, and continues to infringe, the ’237 Patent by using the Accused Instrumentalities. Defendant’s infringement of the ’237 Patent includes, for example, but is not limited to, its use and testing of the Accused Instrumentalities.

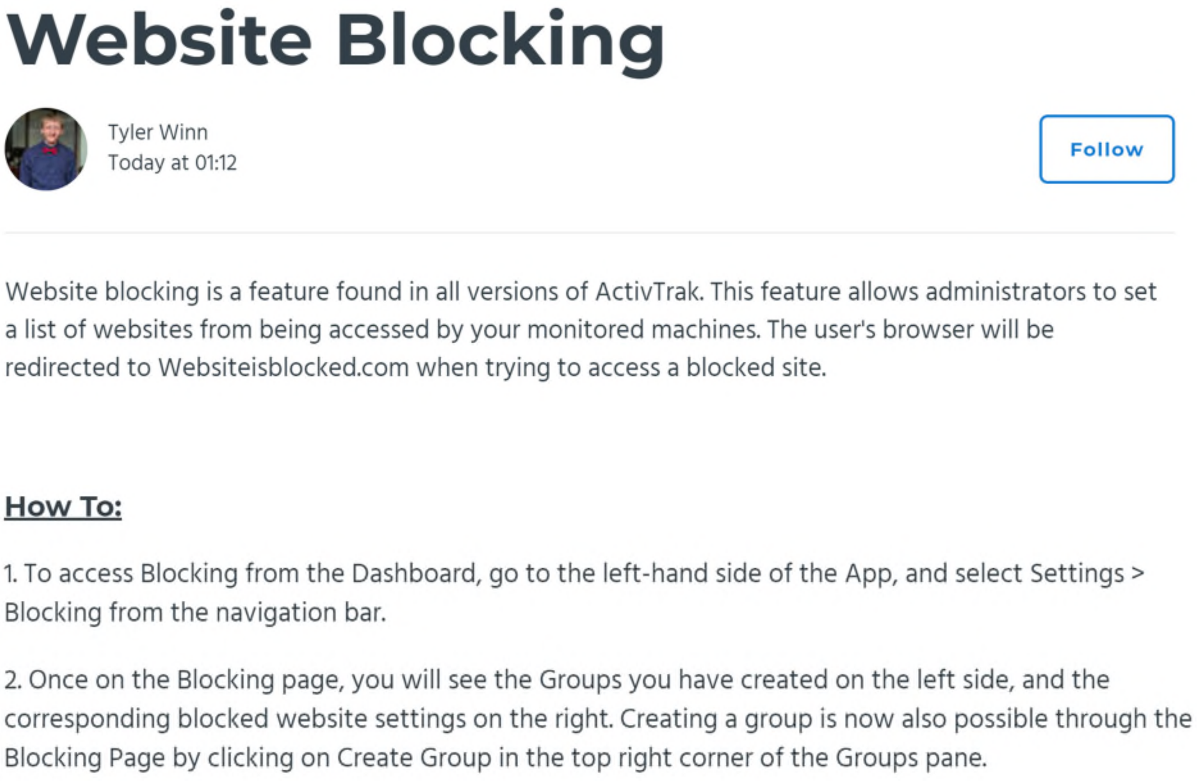
102. On information and belief, Defendant directs or controls its customers to install the Accused Instrumentalities through its websites, including activtrak.com.

103. On information and belief, Defendant also directs or controls its customers to install and use the Accused Instrumentalities through respective application stores for its mobile applications for Apple iOS devices and Android devices.

104. By doing so, Defendant directs or controls its customers to infringe the ’237 Patent by making, having made, using, importing, providing, supplying, distributing, selling, or offering to sell the Accused Instrumentalities in an infringing manner.

105. Defendant, through its own use and testing or its direction or control of its customers, has directly infringed (literally and/or under the doctrine of equivalents) at least Claim 1 of the ’237 Patent. Defendant’s infringement in this regard is ongoing.

106. Through the Accused Instrumentalities, either Defendant or Defendant’s customers under Defendant’s direction or control manage computer network access by, among other things, blocking access to websites.



Website Blocking

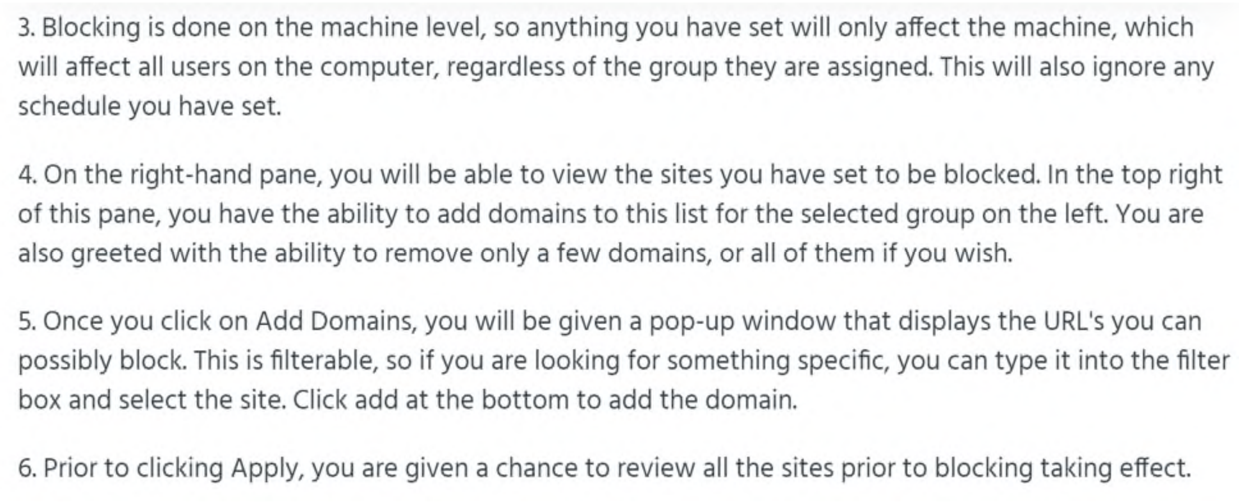
Tyler Winn
Today at 01:12

Website blocking is a feature found in all versions of ActivTrak. This feature allows administrators to set a list of websites from being accessed by your monitored machines. The user's browser will be redirected to Websiteisblocked.com when trying to access a blocked site.

How To:

1. To access Blocking from the Dashboard, go to the left-hand side of the App, and select Settings > Blocking from the navigation bar.

2. Once on the Blocking page, you will see the Groups you have created on the left side, and the corresponding blocked website settings on the right. Creating a group is now also possible through the Blocking Page by clicking on Create Group in the top right corner of the Groups pane.



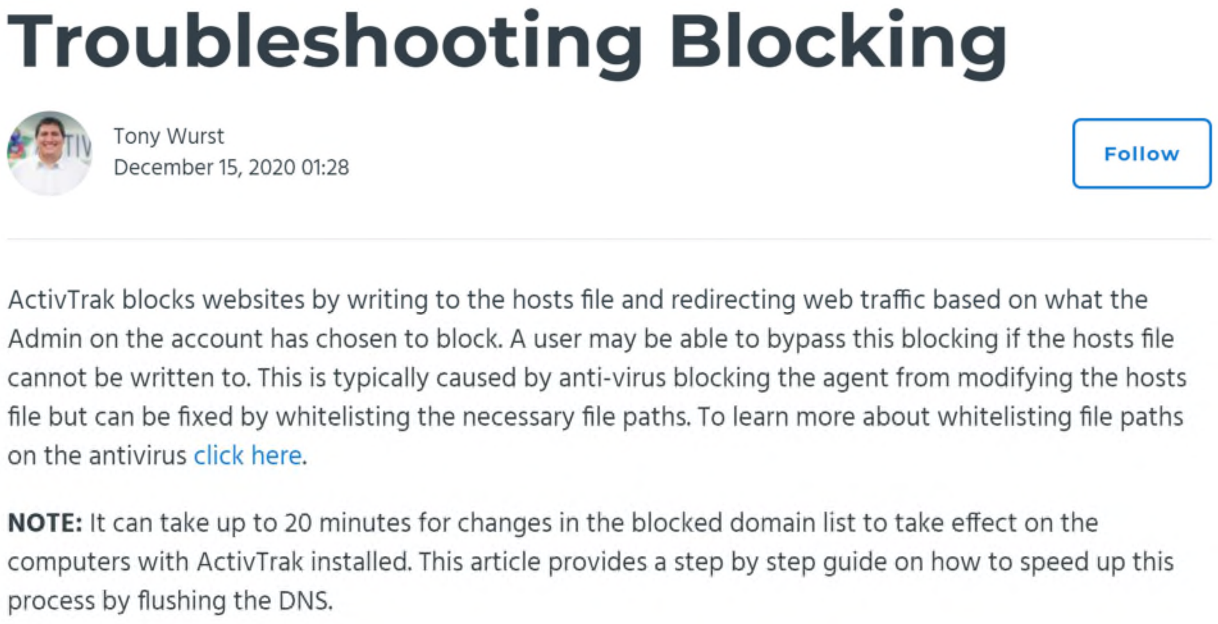
3. Blocking is done on the machine level, so anything you have set will only affect the machine, which will affect all users on the computer, regardless of the group they are assigned. This will also ignore any schedule you have set.

4. On the right-hand pane, you will be able to view the sites you have set to be blocked. In the top right of this pane, you have the ability to add domains to this list for the selected group on the left. You are also greeted with the ability to remove only a few domains, or all of them if you wish.

5. Once you click on Add Domains, you will be given a pop-up window that displays the URL's you can possibly block. This is filterable, so if you are looking for something specific, you can type it into the filter box and select the site. Click add at the bottom to add the domain.

6. Prior to clicking Apply, you are given a chance to review all the sites prior to blocking taking effect.

See https://support.activtrak.com/hc/en-us/articles/360035122372-Website-Blocking



Troubleshooting Blocking

Tony Wurst
December 15, 2020 01:28

ActivTrak blocks websites by writing to the hosts file and redirecting web traffic based on what the Admin on the account has chosen to block. A user may be able to bypass this blocking if the hosts file cannot be written to. This is typically caused by anti-virus blocking the agent from modifying the hosts file but can be fixed by whitelisting the necessary file paths. To learn more about whitelisting file paths on the antivirus click here.

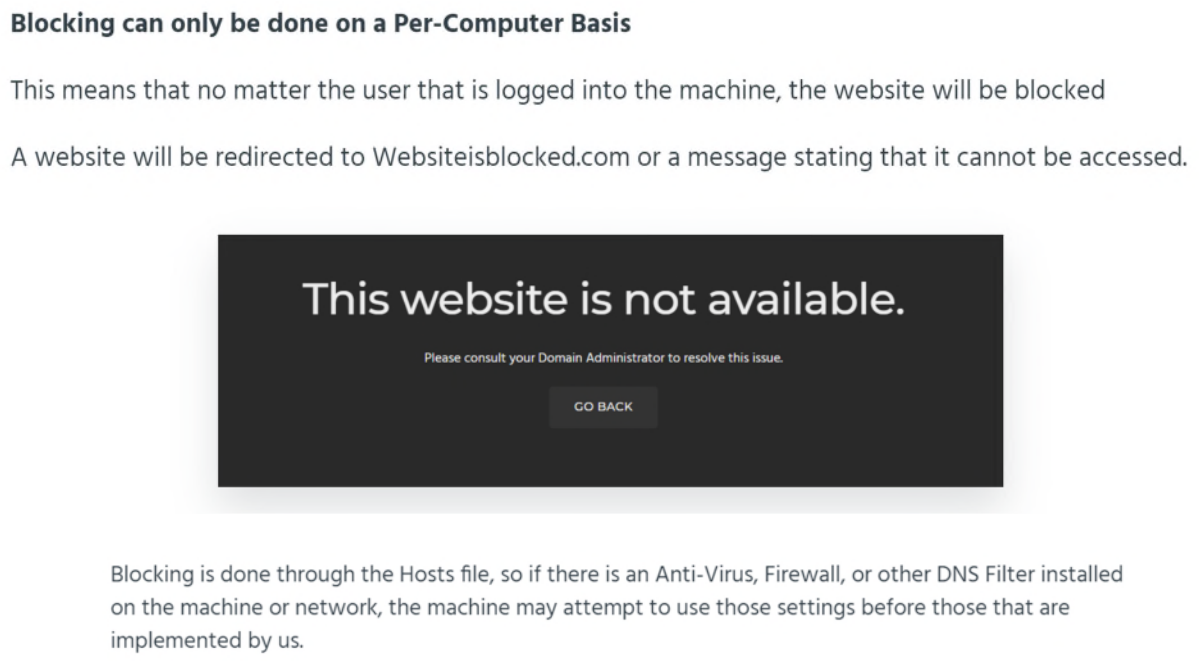
NOTE: It can take up to 20 minutes for changes in the blocked domain list to take effect on the computers with ActivTrak installed. This article provides a step by step guide on how to speed up this process by flushing the DNS.

See https://support.activtrak.com/hc/en-us/articles/360041632051-Troubleshooting-Blocking

107. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control initiate at a client computer a first communication session at a first network address and receive a second network address via the first communication session.

108. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control initiate at the client computer a second communication session at the second network address, through which they receive an access configuration, including a control setting for at least one communication protocol capable of being utilized during a third communication session.

109. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control, instantiate a process on the client computer that instantiates a third communication session and in connection with the third communication session, control the conveyance of data at least one of (i) to and (ii) from the process instantiated on the client computer based on the control setting for the one communication protocol, wherein the one communication protocol is determined from the conveyed data, and the control setting is determined from the thus determined communication protocol.



Blocking can only be done on a Per-Computer Basis

This means that no matter the user that is logged into the machine, the website will be blocked

A website will be redirected to Websiteisblocked.com or a message stating that it cannot be accessed.

This website is not available.

Please consult your Domain Administrator to resolve this issue.

Blocking is done through the Hosts file, so if there is an Anti-Virus, Firewall, or other DNS Filter installed on the machine or network, the machine may attempt to use those settings before those that are implemented by us.

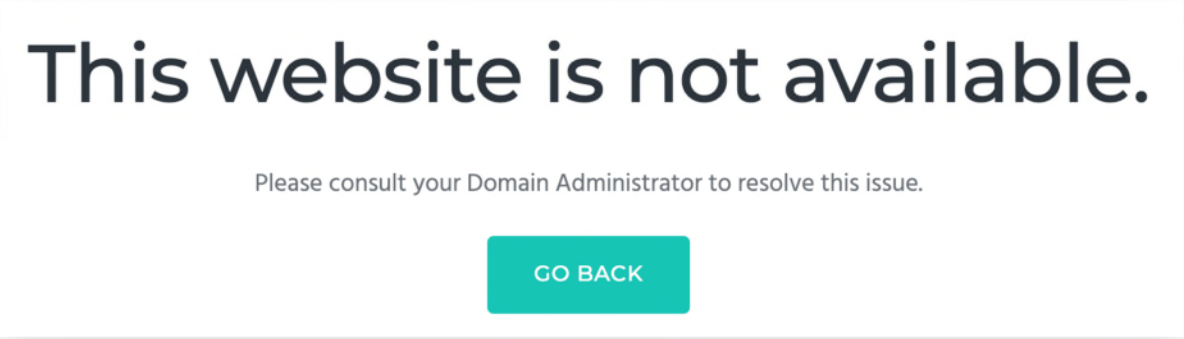
See https://support.activtrak.com/hc/en-us/articles/360037829111-All-You-Need-to-Know-About-Site-Blocking

Resetting the Hosts File

Tony Wurst
December 14, 2020 02:12

Follow

ActivTrak allows administrators to block websites they do not want users accessing.

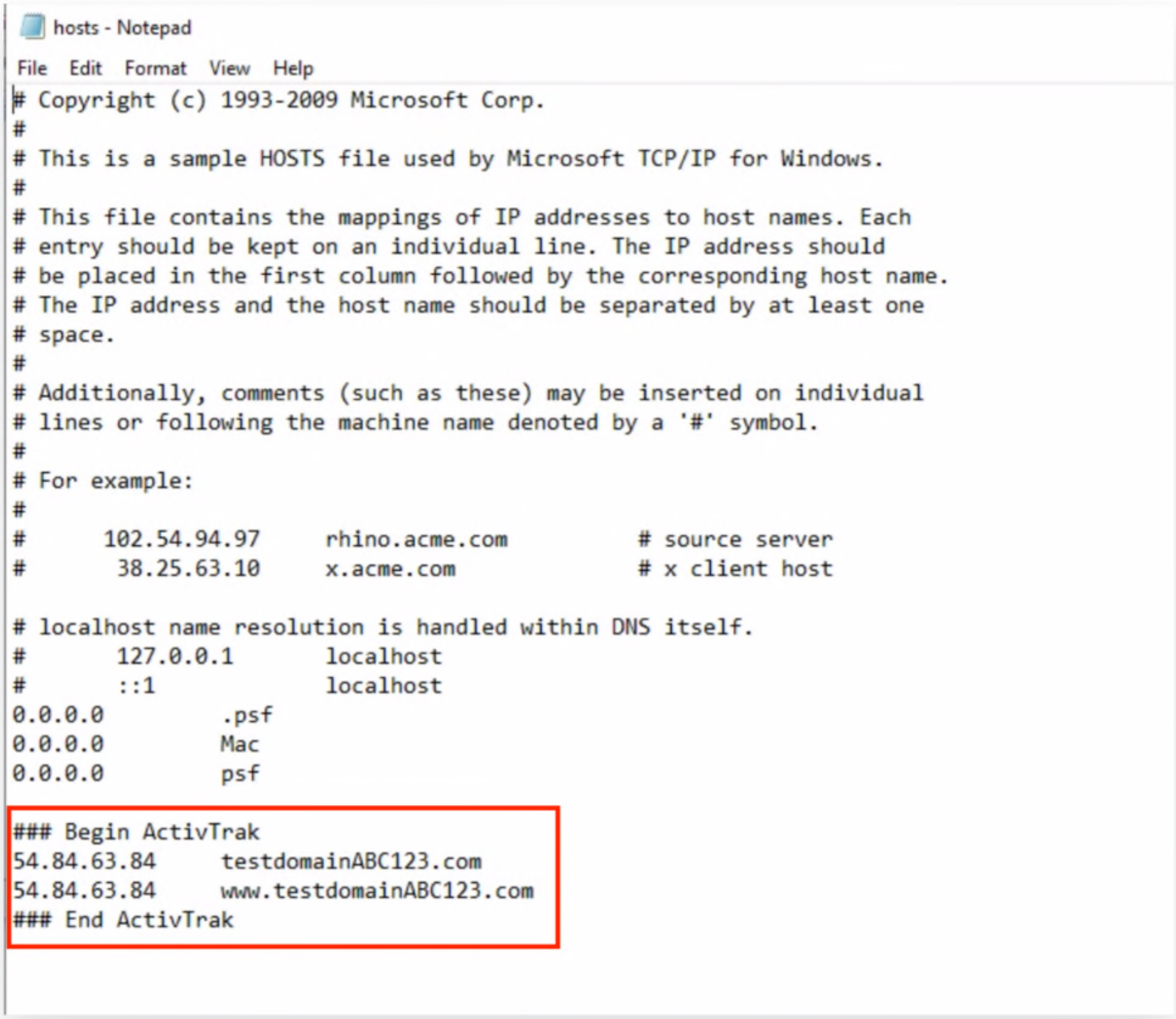


This website is not available.

Please consult your Domain Administrator to resolve this issue.

In order to do this, we make changes to the host file saved on every Mac and PC and use a routing service for the Chrome agent.

Some Anti-Virus agents will prevent ActivTrak from writing to these host files as that can potentially be a security vulnerability. While whitelisting ActivTrak (steps to do this can be found here: https://bit.ly/2RoqugB) will prevent this in most scenarios, it may be necessary to manually remove any blocked websites from this file if your Anti-Virus is preventing the agent from writing to the hosts file.



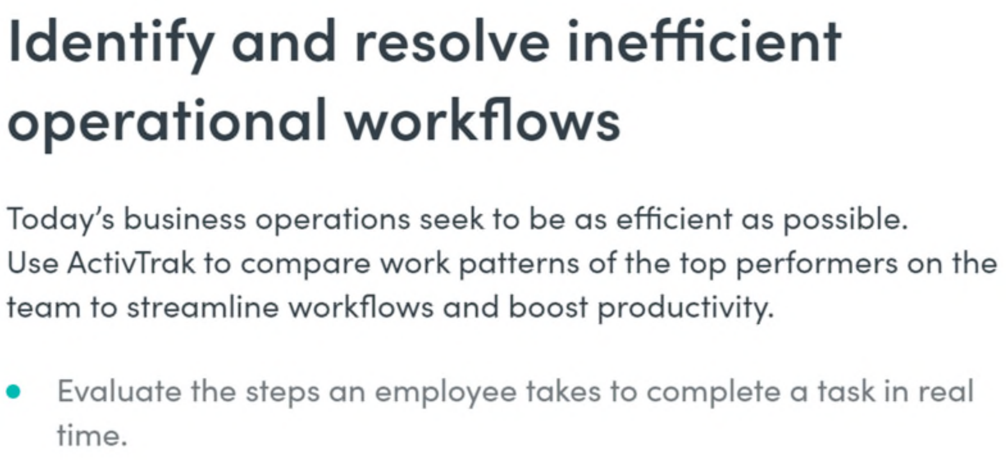
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
0.0.0.0         .psf
0.0.0.0         Mac
0.0.0.0         psf

### Begin ActivTrak
54.84.63.84     testdomainABC123.com
54.84.63.84     www.testdomainABC123.com
### End ActivTrak
```

Everything in between "Begin ActivTrak" and "End ActivTrak" are domains that have been added to the block list on app.activtrak.com and will be blocked by the agent.

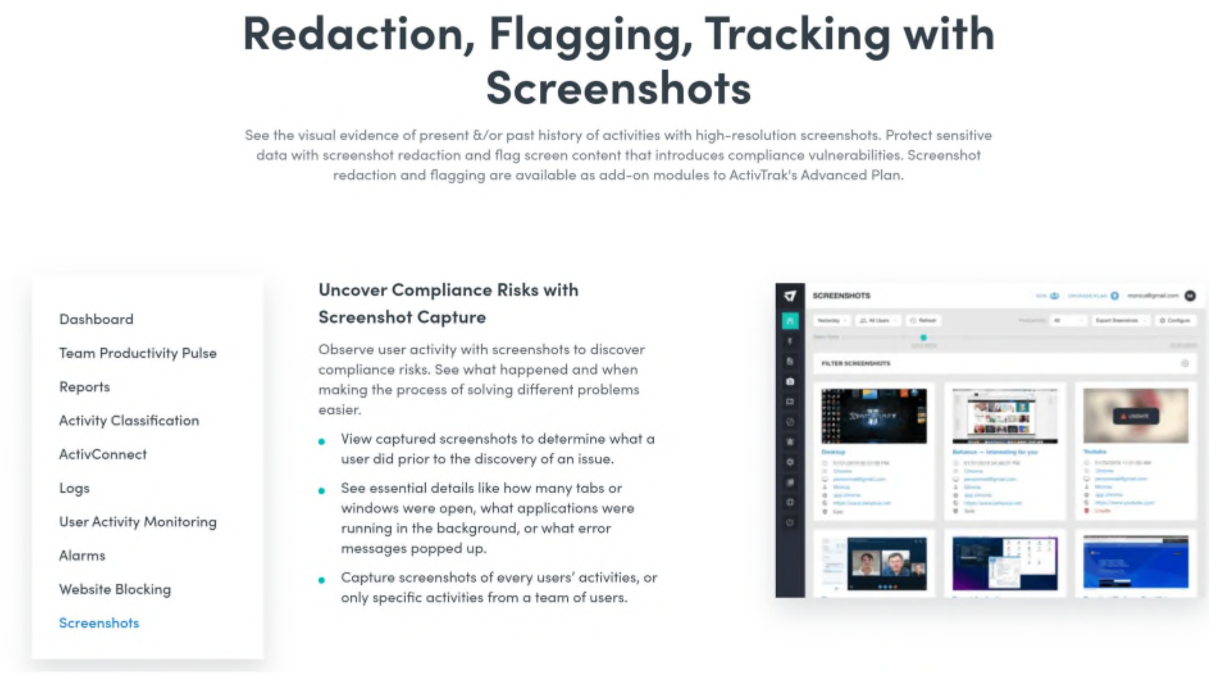
See https://support.activtrak.com/hc/en-us/articles/360038756212-Resetting-the-Hosts-File



Identify and resolve inefficient operational workflows

Today's business operations seek to be as efficient as possible. Use ActivTrak to compare work patterns of the top performers on the team to streamline workflows and boost productivity.

- Evaluate the steps an employee takes to complete a task in real time.



Redaction, Flagging, Tracking with Screenshots

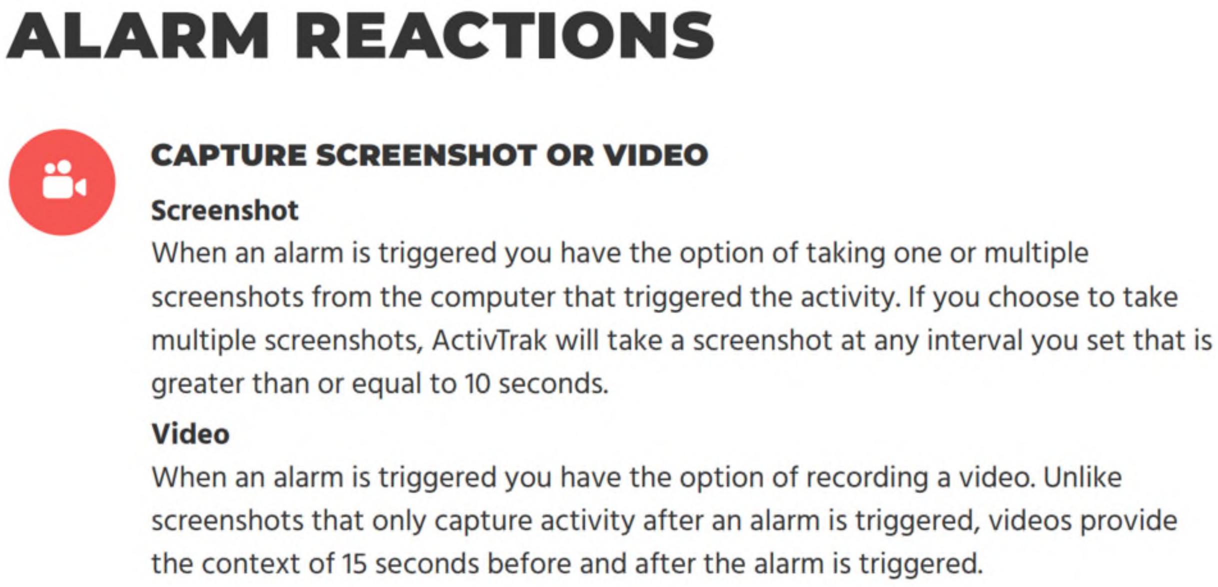
See the visual evidence of present &/or past history of activities with high-resolution screenshots. Protect sensitive data with screenshot redaction and flag screen content that introduces compliance vulnerabilities. Screenshot redaction and flagging are available as add-on modules to ActivTrak's Advanced Plan.

Uncover Compliance Risks with Screenshot Capture

Observe user activity with screenshots to discover compliance risks. See what happened and when making the process of solving different problems easier.

- View captured screenshots to determine what a user did prior to the discovery of an issue.
- See essential details like how many tabs or windows were open, what applications were running in the background, or what error messages popped up.
- Capture screenshots of every users' activities, or only specific activities from a team of users.

See https://activtrak.com/product/screenshots/



ALARM REACTIONS

CAPTURE SCREENSHOT OR VIDEO

Screenshot

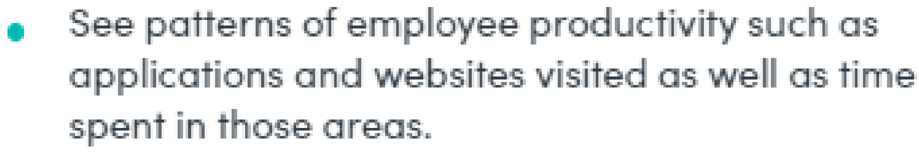
When an alarm is triggered you have the option of taking one or multiple screenshots from the computer that triggered the activity. If you choose to take multiple screenshots, ActivTrak will take a screenshot at any interval you set that is greater than or equal to 10 seconds.

Video

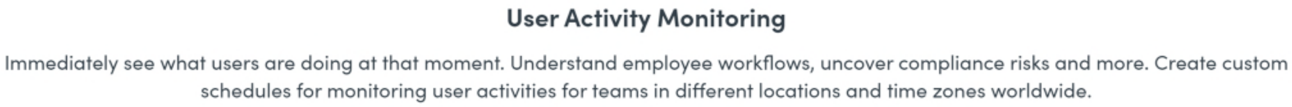
When an alarm is triggered you have the option of recording a video. Unlike screenshots that only capture activity after an alarm is triggered, videos provide the context of 15 seconds before and after the alarm is triggered.

See https://3k9e724pnqn2ubftz25jfqs4-wpengine.netdna-ssl.com/wp-content/uploads/2019/08/ALARMS_%E2%80%94new_logo.pdf

110. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control transfer at least part of the conveyed data to the second network address (which is under Defendant's control) via the second communication session.



- See patterns of employee productivity such as applications and websites visited as well as time spent in those areas.



User Activity Monitoring

Immediately see what users are doing at that moment. Understand employee workflows, uncover compliance risks and more. Create custom schedules for monitoring user activities for teams in different locations and time zones worldwide.

https://activtrak.com/product/logs/

111. Plaintiff has been damaged as a result of the infringing conduct by Defendant or Defendant's customers under Defendant's control alleged above. Thus, Defendant is liable to Plaintiff in an amount that adequately compensates it for such infringements, which by law cannot

be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

112. Plaintiff and/or its predecessors-in-interest have satisfied all statutory obligations required to collect pre-filing damages for the full period allowed by law for infringement of the ’237 Patent.

Indirect Infringement

113. Plaintiff repeats and re-alleges the allegations in Paragraphs 1-112 as though fully set forth in their entirety.

114. Defendant has also indirectly infringed the ’237 Patent, at least since the filing of this complaint, by inducing others to directly infringe the ’237 Patent. Defendant has induced others, including its customers, affiliates, third-party manufacturers, shippers, distributors, retailers, or other persons acting on Defendant’s or its affiliates’ behalf, to directly infringe (literally and/or under the doctrine of equivalents) the ’237 Patent by making, having made, using, importing, providing, supplying, distributing, selling, or offering to sell the Accused Instrumentalities in an infringing manner. Defendant took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to, for example, use the Accused Instrumentalities in a manner that infringes one or more claims of the ’237 Patent or induce others to use the Accused Instrumentalities in a manner that infringes one or more claims of the ’237 Patent, including, for example, Claim 1 of the ’237 Patent. Such steps by Defendant included, among other things, advising or directing others to use the Accused Instrumentalities in an infringing manner; advertising and promoting the use of the Accused Instrumentalities in an infringing manner; and/or distributing instructions that guide others to use, operate, make, or have made the Accused Instrumentalities in an infringing manner. Defendant is performing these steps,

which constitute induced infringement, with the knowledge of the ’237 Patent and with the knowledge that the induced acts constitute infringement. Defendant’s inducement is ongoing.

115. Defendant has also indirectly infringed by contributing to the infringement of the ’237 Patent. Defendant has contributed to the direct infringement of the ’237 Patent by its customers, affiliates, or third-party manufacturers, shippers, distributors, retailers, or other persons acting on its or its affiliates’ behalf. The Accused Instrumentalities have special features that are specially designed to be used in an infringing way and that have no substantial uses other than ones that infringe the ’237 Patent, including, for example, Claim 1 of the ’237 Patent. The special features include, for example, the manage computer-network-access management by blocking access to websites that is used in a manner that infringes the Asserted Patents. The special features constitute a material part of the invention of one or more of the claims of the ’237 Patent and are not staple articles of commerce suitable for substantial non-infringing use. Defendant’s contributory infringement is ongoing.

116. Defendant has knowledge of the ’237 Patent at least as of the date when it was notified of the filing of this action.

117. Defendant’s actions are at least objectively reckless as to the risk of infringing a valid patent and this objective risk was either known or should have been known by Defendant.

118. Defendant’s direct and indirect infringement of the ’237 Patent is, has been, and continues to be willful, intentional, deliberate, and/or in conscious disregard of Plaintiff’s rights under the patent.

119. Plaintiff has been damaged as a result of the infringing conduct by Defendant alleged above. Thus, Defendant is liable to Weserve in an amount that adequately compensates it

for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT IV: INFRINGEMENT OF U.S. PATENT NO. 8,930,535

Direct Infringement

120. Plaintiff repeats and re-alleges the allegations in Paragraphs 1-119 as if fully set forth in their entirety.

121. On January 6, 2015, the ’535 Patent was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Method for Managing Computer Network Access.”

122. Exhibit D is a true and correct copy of the ’535 Patent.

123. Plaintiff is the owner of the ’535 Patent, with all substantial rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the ’535 Patent against infringers, and to collect damages for all relevant times.

124. The ’535 Patent describes novel and non-obvious methods of remotely monitoring an Internet session.

125. The claims of the ’535 Patent are not directed to an abstract idea.

126. For example, Claim 4 is a technical improvement over prior-art methods of controlling computer network access.

127. Claim 4 recites “controlling computer network access” in which a client computer initiates a communication session to receive a network address that is used to receive “an access configuration including a control setting for at least one communication protocol capable of being utilized during a monitored communication session.” The client computer initiates “a monitored communication session at a network address,” during which the client computer controls the conveyance of data “at least one of (i) to and (ii) from the process instantiated on the client

computer based on the control setting for the one communication protocol, wherein the one communication protocol is determined from the conveyed data or client communication application, and the control setting is obtained by the client computer from the access configuration." At least part of the conveyed data is transferred to a network data server. Claim 4 does not recite an abstract idea because it recites specific conditions and information used to control computer network access.

128. Prior-art systems and methods did not include the ability to control computer network access in the manner described and claimed in at least Claim 4.

129. Regardless of whether Claim 4 is directed to an abstract idea, Claim 4 recites patentable subject matter because it recites an inventive concept.

130. For example, the patented method for managing computer network access was not a well-understood practice, routine, or conventional; rather it represents an improvement to computing technology that allows for superior security for online communications.

131. Moreover, the use of the components recited in Claim 4 was, at the time of the invention, unconventional; therefore, Claim 4 recites an inventive concept.

132. The written description of the '535 Patent describes in technical detail each of the limitations of the claims, allowing a skilled artisan to understand the scope of the claims and how the non-conventional and non-generic combination of claim limitations is patentably distinct from and improved upon what may have been considered conventional or generic in the art at the time of the invention.

133. Defendant made, had made, used, imported, provided, supplied, distributed, sold, or offered to sell the Accused Instrumentalities.

134. Defendant has infringed, and continues to infringe, the ’535 Patent by using the Accused Instrumentalities. Defendant’s infringement of the ’535 Patent includes, for example, but is not limited to, its use and testing of the Accused Instrumentalities.

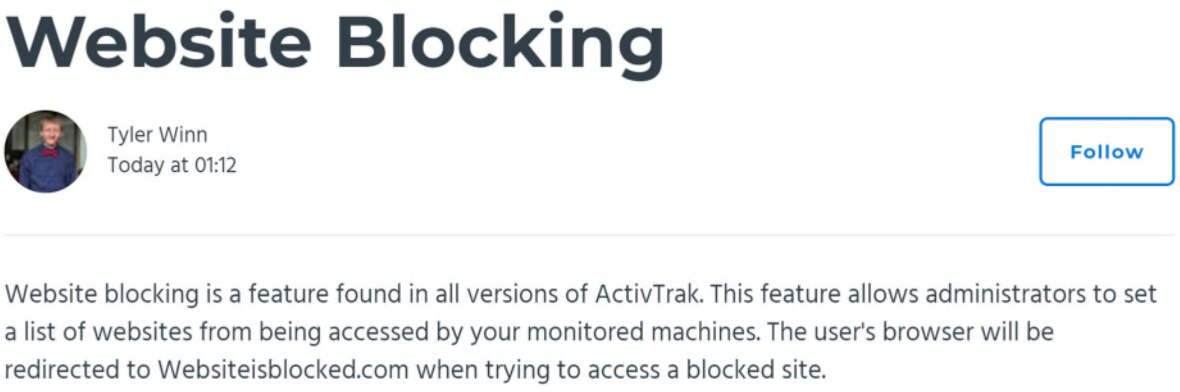
135. On information and belief, Defendant directs or controls its customers to install the Accused Instrumentalities through its websites, including activtrak.com.

136. On information and belief, Defendant also directs or controls its customers to install and use the Accused Instrumentalities through respective application stores for its mobile applications for Apple iOS devices and Android devices.

137. By doing so, Defendant directs or controls its customers to infringe the ’535 Patent by making, having made, using, importing, providing, supplying, distributing, selling, or offering to sell the Accused Instrumentalities in an infringing manner.

138. Defendant, through its own use and testing or its direction or control of its customers, has directly infringed (literally and/or under the doctrine of equivalents) at least Claim 4 of the ’535 Patent. Defendant’s infringement in this regard is ongoing.

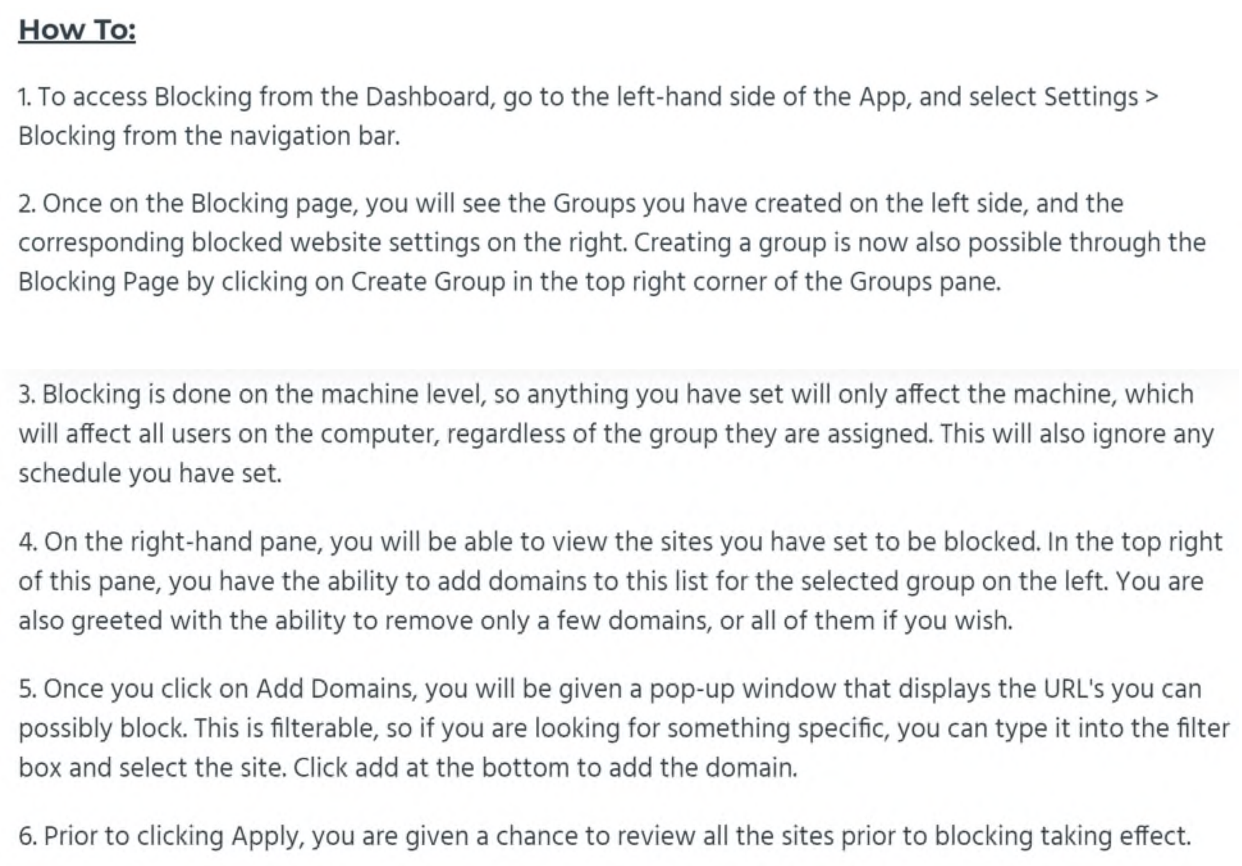
139. Through the Accused Instrumentalities, either Defendant or Defendant’s customers under Defendant’s direction or control, control computer network access by, among other things, blocking access to websites.



Website Blocking

Tyler Winn
Today at 01:12

Website blocking is a feature found in all versions of ActivTrak. This feature allows administrators to set a list of websites from being accessed by your monitored machines. The user's browser will be redirected to Websiteisblocked.com when trying to access a blocked site.



How To:

1. To access Blocking from the Dashboard, go to the left-hand side of the App, and select Settings > Blocking from the navigation bar.

2. Once on the Blocking page, you will see the Groups you have created on the left side, and the corresponding blocked website settings on the right. Creating a group is now also possible through the Blocking Page by clicking on Create Group in the top right corner of the Groups pane.

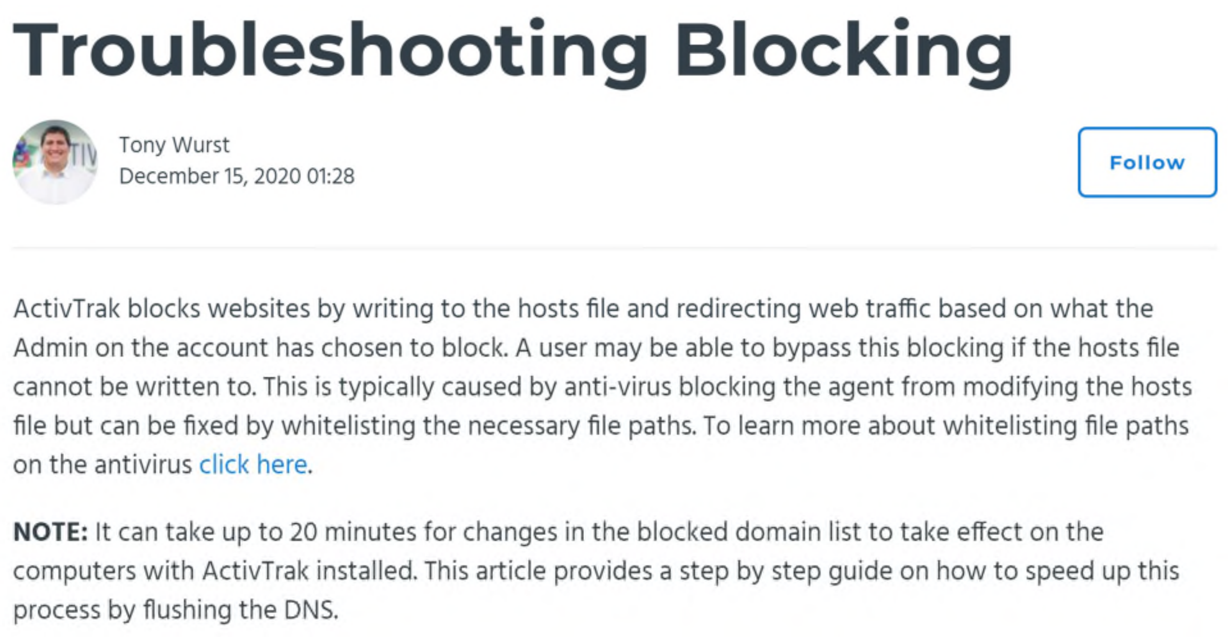
3. Blocking is done on the machine level, so anything you have set will only affect the machine, which will affect all users on the computer, regardless of the group they are assigned. This will also ignore any schedule you have set.

4. On the right-hand pane, you will be able to view the sites you have set to be blocked. In the top right of this pane, you have the ability to add domains to this list for the selected group on the left. You are also greeted with the ability to remove only a few domains, or all of them if you wish.

5. Once you click on Add Domains, you will be given a pop-up window that displays the URL's you can possibly block. This is filterable, so if you are looking for something specific, you can type it into the filter box and select the site. Click add at the bottom to add the domain.

6. Prior to clicking Apply, you are given a chance to review all the sites prior to blocking taking effect.

See https://support.activtrak.com/hc/en-us/articles/360035122372-Website-Blocking



Troubleshooting Blocking

Tony Wurst
December 15, 2020 01:28

ActivTrak blocks websites by writing to the hosts file and redirecting web traffic based on what the Admin on the account has chosen to block. A user may be able to bypass this blocking if the hosts file cannot be written to. This is typically caused by anti-virus blocking the agent from modifying the hosts file but can be fixed by whitelisting the necessary file paths. To learn more about whitelisting file paths on the antivirus click here.

NOTE: It can take up to 20 minutes for changes in the blocked domain list to take effect on the computers with ActivTrak installed. This article provides a step by step guide on how to speed up this process by flushing the DNS.

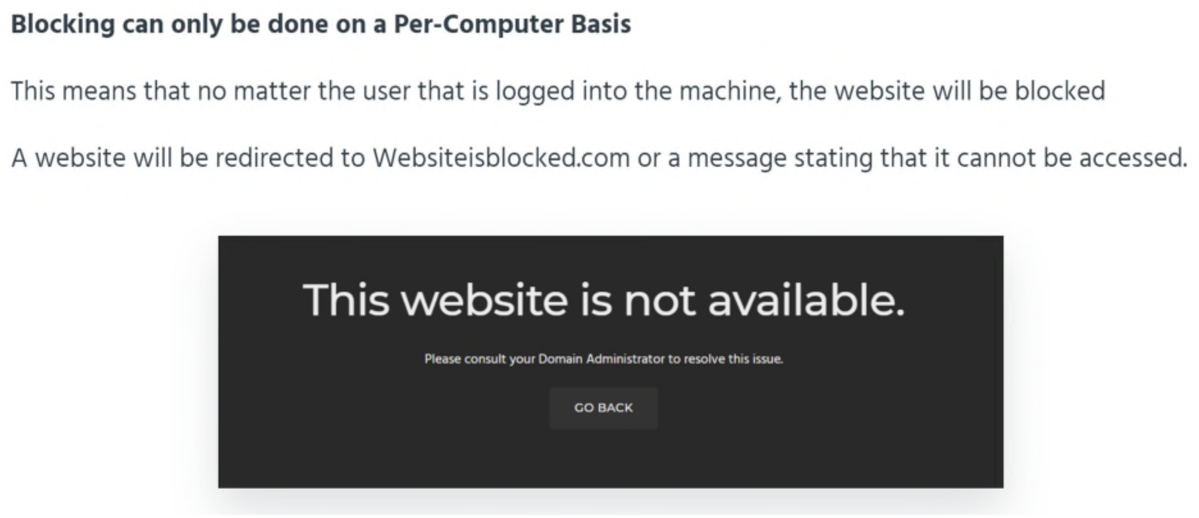
See https://support.activtrak.com/hc/en-us/articles/360041632051-Troubleshooting-Blocking

140. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control initiate at a client computer a communication session at a network primary server.

141. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control receive at the client computer via the network primary communication server communication session a network address for a network data server.

142. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control initiate at the client computer a communication session with the network data server.

143. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control receive at the client computer from the network primary server an access configuration including a control setting for at least one communication protocol capable of being utilized during a monitored communication session.



Blocking can only be done on a Per-Computer Basis

This means that no matter the user that is logged into the machine, the website will be blocked

A website will be redirected to Websiteisblocked.com or a message stating that it cannot be accessed.

This website is not available.

Please consult your Domain Administrator to resolve this issue.

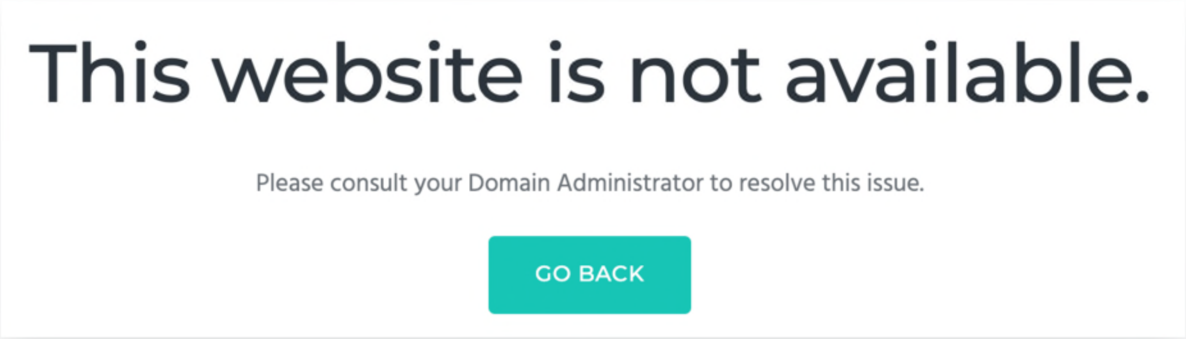
See https://support.activtrak.com/hc/en-us/articles/360037829111-All-You-Need-to-Know-About-Site-Blocking

Resetting the Hosts File

Tony Wurst
December 14, 2020 02:12

Follow

ActivTrak allows administrators to block websites they do not want users accessing.

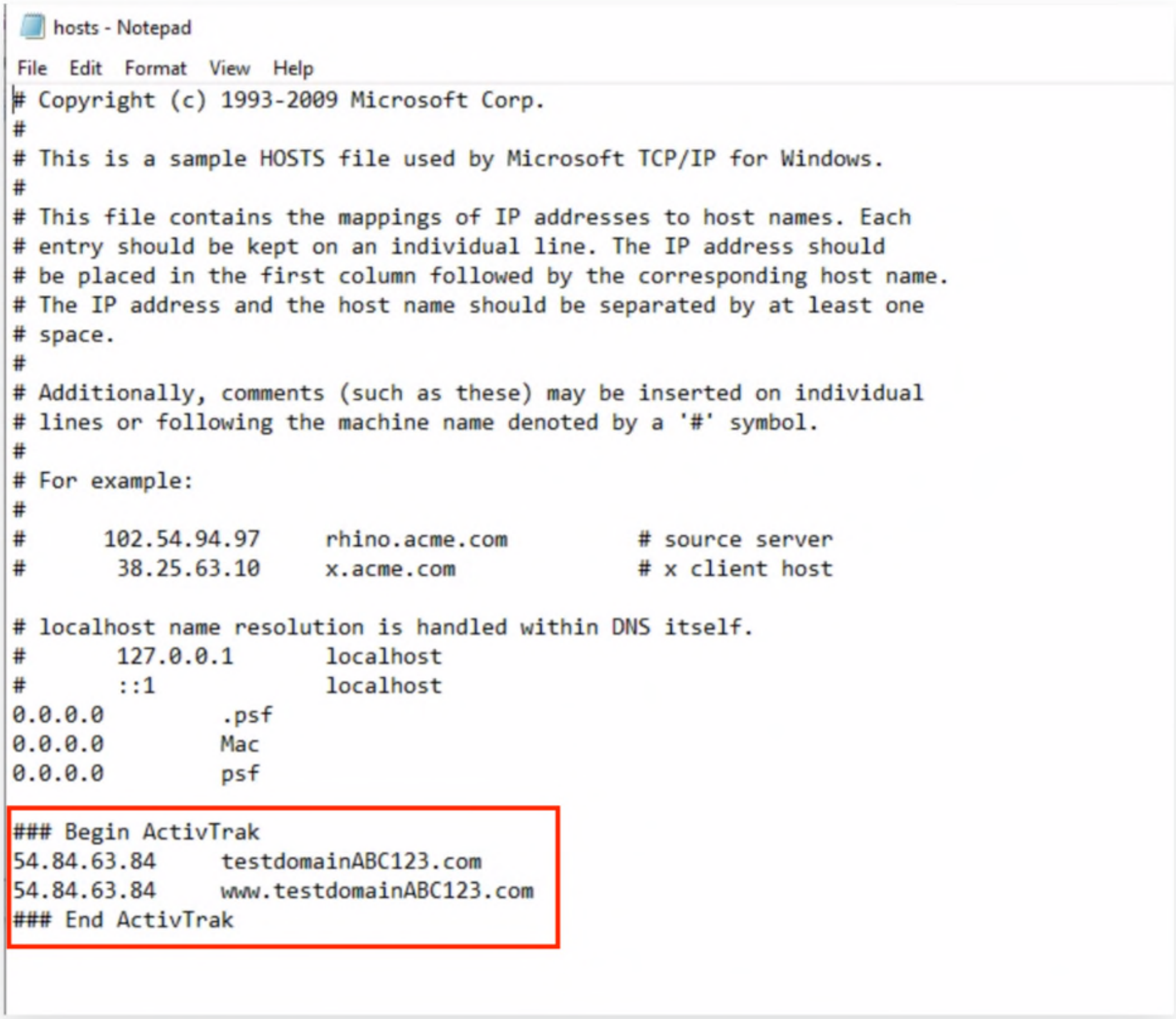


This website is not available.

Please consult your Domain Administrator to resolve this issue.

In order to do this, we make changes to the host file saved on every Mac and PC and use a routing service for the Chrome agent.

Some Anti-Virus agents will prevent ActivTrak from writing to these host files as that can potentially be a security vulnerability. While whitelisting ActivTrak (steps to do this can be found here: https://bit.ly/2RoqugB) will prevent this in most scenarios, it may be necessary to manually remove any blocked websites from this file if your Anti-Virus is preventing the agent from writing to the hosts file.



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
0.0.0.0         .psf
0.0.0.0         Mac
0.0.0.0         psf

### Begin ActivTrak
54.84.63.84     testdomainABC123.com
54.84.63.84     www.testdomainABC123.com
### End ActivTrak
```

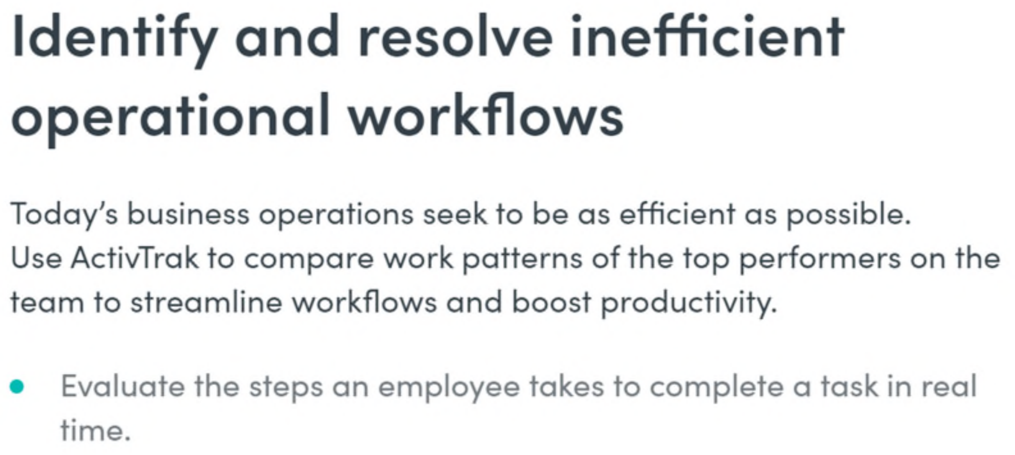
Everything in between "Begin ActivTrak" and "End ActivTrak" are domains that have been added to the block list on app.activtrak.com and will be blocked by the agent.

See https://support.activtrak.com/hc/en-us/articles/360038756212-Resetting-the-Hosts-File

144. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control, instantiate at the client computer a process which initiates a monitored communication session at a network address.

145. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control, in connection with the monitored communication session, control the conveyance of data at least one of (i) to and (ii) from the process instantiated on the

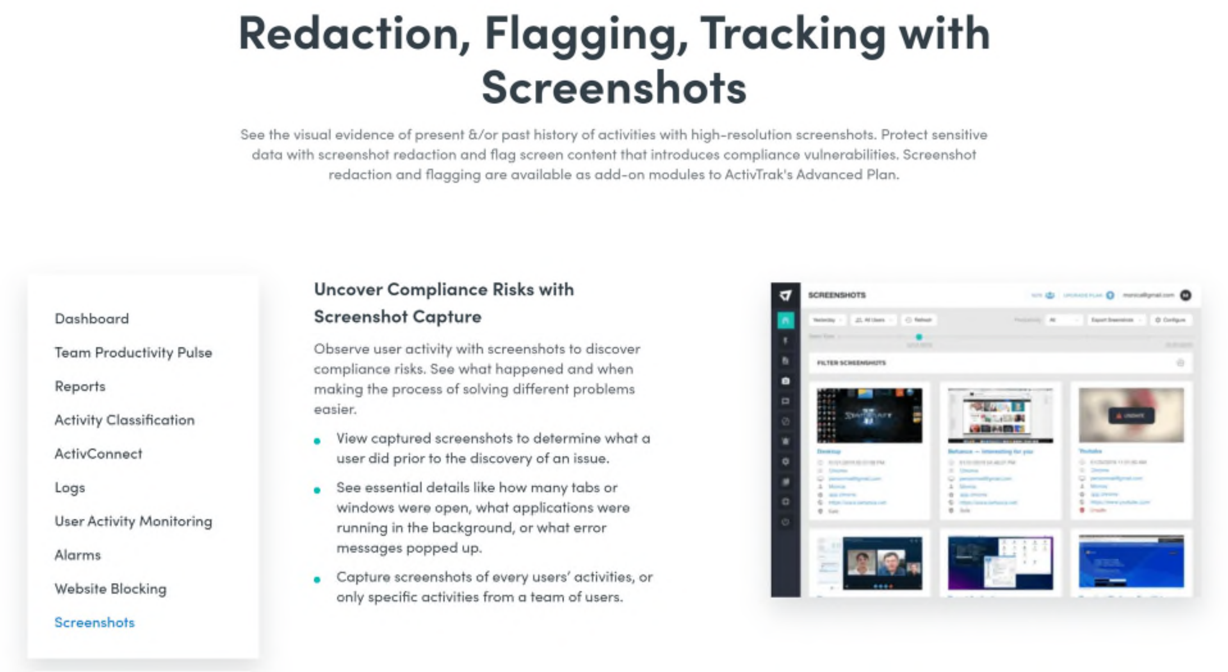
client computer based on the control setting for the one communication protocol, wherein the one communication protocol is determined from the conveyed data or client communication application, and the control setting is obtained by the client computer from the access configuration.



Identify and resolve inefficient operational workflows

Today's business operations seek to be as efficient as possible. Use ActivTrak to compare work patterns of the top performers on the team to streamline workflows and boost productivity.

- Evaluate the steps an employee takes to complete a task in real time.



Redaction, Flagging, Tracking with Screenshots

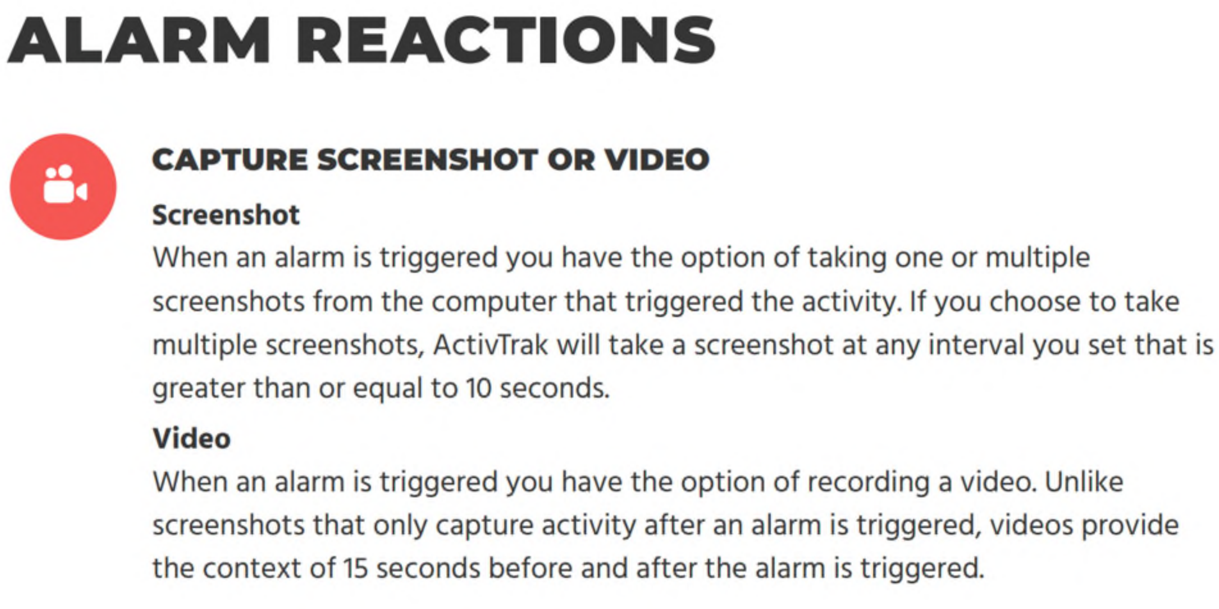
See the visual evidence of present &/or past history of activities with high-resolution screenshots. Protect sensitive data with screenshot redaction and flag screen content that introduces compliance vulnerabilities. Screenshot redaction and flagging are available as add-on modules to ActivTrak's Advanced Plan.

Uncover Compliance Risks with Screenshot Capture

Observe user activity with screenshots to discover compliance risks. See what happened and when making the process of solving different problems easier.

- View captured screenshots to determine what a user did prior to the discovery of an issue.
- See essential details like how many tabs or windows were open, what applications were running in the background, or what error messages popped up.
- Capture screenshots of every users' activities, or only specific activities from a team of users.

See https://activtrak.com/product/screenshots/



ALARM REACTIONS

CAPTURE SCREENSHOT OR VIDEO

Screenshot

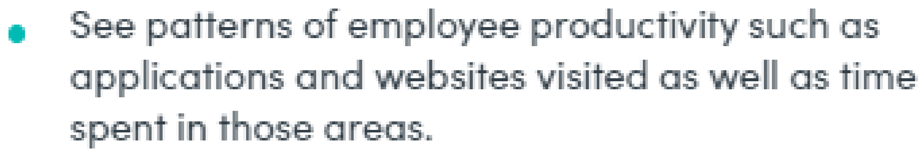
When an alarm is triggered you have the option of taking one or multiple screenshots from the computer that triggered the activity. If you choose to take multiple screenshots, ActivTrak will take a screenshot at any interval you set that is greater than or equal to 10 seconds.

Video

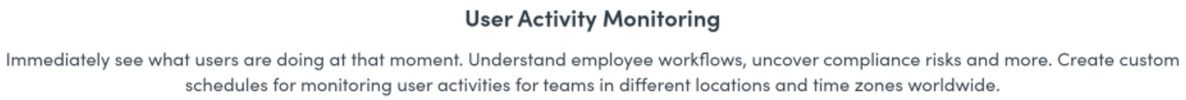
When an alarm is triggered you have the option of recording a video. Unlike screenshots that only capture activity after an alarm is triggered, videos provide the context of 15 seconds before and after the alarm is triggered.

See https://3k9e724pnqn2ubftz25jfqs4-wpengine.netdna-ssl.com/wp-content/uploads/2019/08/ALARMS_%E2%80%94new_logo.pdf

146. Through the Accused Instrumentalities, either Defendant or Defendant's customers under Defendant's direction or control transfer at least part of the conveyed data to the network data server via the communication session between the client computer and the network data server.



- See patterns of employee productivity such as applications and websites visited as well as time spent in those areas.



User Activity Monitoring

Immediately see what users are doing at that moment. Understand employee workflows, uncover compliance risks and more. Create custom schedules for monitoring user activities for teams in different locations and time zones worldwide.

See https://activtrak.com/product/logs/

147. Plaintiff has been damaged as a result of the infringing conduct by Defendant or Defendant's customers under Defendant's control alleged above. Thus, Defendant is liable to

Plaintiff in an amount that adequately compensates it for such infringements, which by law cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

148. Plaintiff and/or its predecessors-in-interest have satisfied all statutory obligations required to collect pre-filing damages for the full period allowed by law for infringement of the ’535 Patent.

Indirect Infringement

149. Plaintiff repeats and re-alleges the allegations in Paragraphs 1-148 as though fully set forth in their entirety.

150. Defendant has also indirectly infringed the ’535 Patent, at least since the filing of this complaint, by inducing others to directly infringe the ’535 Patent. Defendant has induced others, including its customers, affiliates, third-party manufacturers, shippers, distributors, retailers, or other persons acting on Defendant’s or its affiliates’ behalf, to directly infringe (literally and/or under the doctrine of equivalents) the ’535 Patent by making, having made, using, importing, providing, supplying, distributing, selling, or offering to sell the Accused Instrumentalities in an infringing manner. Defendant took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to, for example, use the Accused Instrumentalities in a manner that infringes one or more claims of the ’535 Patent or induce other to use the Accused Instrumentalities in a manner that infringes one or more claims of the ’535 Patent, including, for example, Claim 4 of the ’535 Patent. Such steps by Defendant included, among other things, advising or directing others to use the Accused Instrumentalities in an infringing manner; advertising and promoting the use of the Accused Instrumentalities in an infringing manner; and/or distributing instructions that guide others to use, operate, make, or have

made the Accused Instrumentalities in an infringing manner. Defendant is performing these steps, which constitute induced infringement with the knowledge of the ’535 Patent and with the knowledge that the induced acts constitute infringement. Defendant’s inducement is ongoing.

151. Defendant has also indirectly infringed by contributing to the infringement of the ’535 Patent. Defendant has contributed to the direct infringement of the ’535 Patent by its customers, affiliates, or third-party manufacturers, shippers, distributors, retailers, or other persons acting on its or its affiliates’ behalf. The Accused Instrumentalities have special features that are specially designed to be used in an infringing way and that have no substantial uses other than ones that infringe the ’535 Patent, including, for example, Claim 4 of the ’535 Patent. The special features include, for example, controlling computer network access that is used in a manner that infringes the Asserted Patents. The special features constitute a material part of the invention of one or more of the claims of the ’535 Patent and are not staple articles of commerce suitable for substantial non-infringing use. Defendant’s contributory infringement is ongoing.

152. Defendant has knowledge of the ’535 Patent at least as of the date when it was notified of the filing of this action.

153. Defendant’s actions are at least objectively reckless as to the risk of infringing a valid patent and this objective risk was either known or should have been known by Defendant.

154. Defendant’s direct and indirect infringement of the ’535 Patent is, has been, and continues to be willful, intentional, deliberate, and/or in conscious disregard of Plaintiff’s rights under the patent.

155. Plaintiff has been damaged as a result of the infringing conduct by Defendant alleged above. Thus, Defendant is liable to Weserve in an amount that adequately compensates it

for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

Plaintiff hereby requests a trial by jury on all issues so triable by right.

PRAYER FOR RELIEF

Weserve requests that the Court find in its favor and against Defendant, and that the Court grant Weserve the following relief:

a. Judgment that one or more claims of the Asserted Patents have been infringed, either literally and/or under the doctrine of equivalents, by Defendant and/or all others acting in concert therewith;

b. A permanent injunction enjoining Defendant and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert therewith from infringement of the Asserted Patents; or, in the alternative, an award of a reasonable ongoing royalty for future infringement of the Asserted Patents by such entities;

c. Judgment that Defendant accounts for and pays to Weserve all damages to and costs incurred by Weserve because of Defendant's infringing activities and other conduct complained of herein;

d. Judgment that Defendant's infringements be found willful, and that the Court award treble damages for the period of such willful infringement pursuant to 35 U.S.C. § 284;

e. That Weserve be granted pre-judgment and post-judgment interest on the damages caused by Defendant's infringing activities and other conduct complained of herein;

f. That this Court declare this an exceptional case and award Weserve its reasonable attorney's fees and costs in accordance with 35 U.S.C. § 285; and

g. That Weserve be granted such other and further relief as the Court may deem just and proper under the circumstances.

Dated: March 10, 2021

Respectfully submitted,

By: /s/ Fred I. Williams
Fred I. Williams
Texas State Bar No. 00794855
Michael Simons
Texas State Bar No. 24008042
Jonathan L. Hardt
Texas State Bar No. 24039906
WILLIAMS SIMONS & LANDIS PLLC
327 Congress Ave., Suite 490
Austin, TX 78701
Tel: 512-543-1354
fwilliams@wsltrial.com
msimons@wsltrial.com
jhardt@wsltrial.com

Todd E. Landis (*pro hac vice* pending)
State Bar No. 24030226
WILLIAMS SIMONS & LANDIS PLLC
2633 McKinney Ave., Suite 130 #366
Dallas, TX 75204
Tel: 512-543-1357
tlandis@wsltrial.com

John Wittenzellner
Pennsylvania State Bar No. 308996
WILLIAMS SIMONS & LANDIS PLLC
1735 Market Street, Suite A #453
Philadelphia, PA 19103
Tel: 512-543-1373
johnw@wsltrial.com

Attorneys for Plaintiff Weserve Access, LLC